

INTERROGATION



BERSERKER

BOOKS



Jack Luger

This book is sold for information purposes only. Neither the author nor the publisher will be held accountable for the use or misuse of the information contained in this book.

ASK ME NO QUESTIONS, I'LL TELL YOU NO LIES: How to Survive Being Interviewed, Interrogated, Questioned, Quizzed, Sweated, Grilled...

© 1991 by Jack Luger

Printed in USA

All rights reserved. No part of this book may be reproduced or stored in any form whatsoever without the prior written consent of the publisher. Reviews may quote brief passages without the written consent of the publisher as long as proper credit is given.

Published by:

Loompanics Unlimited

PO Box 1197

Port Townsend, WA 98368

Loompanics Unlimited is a Division of Loompanics Enterprises, Inc.

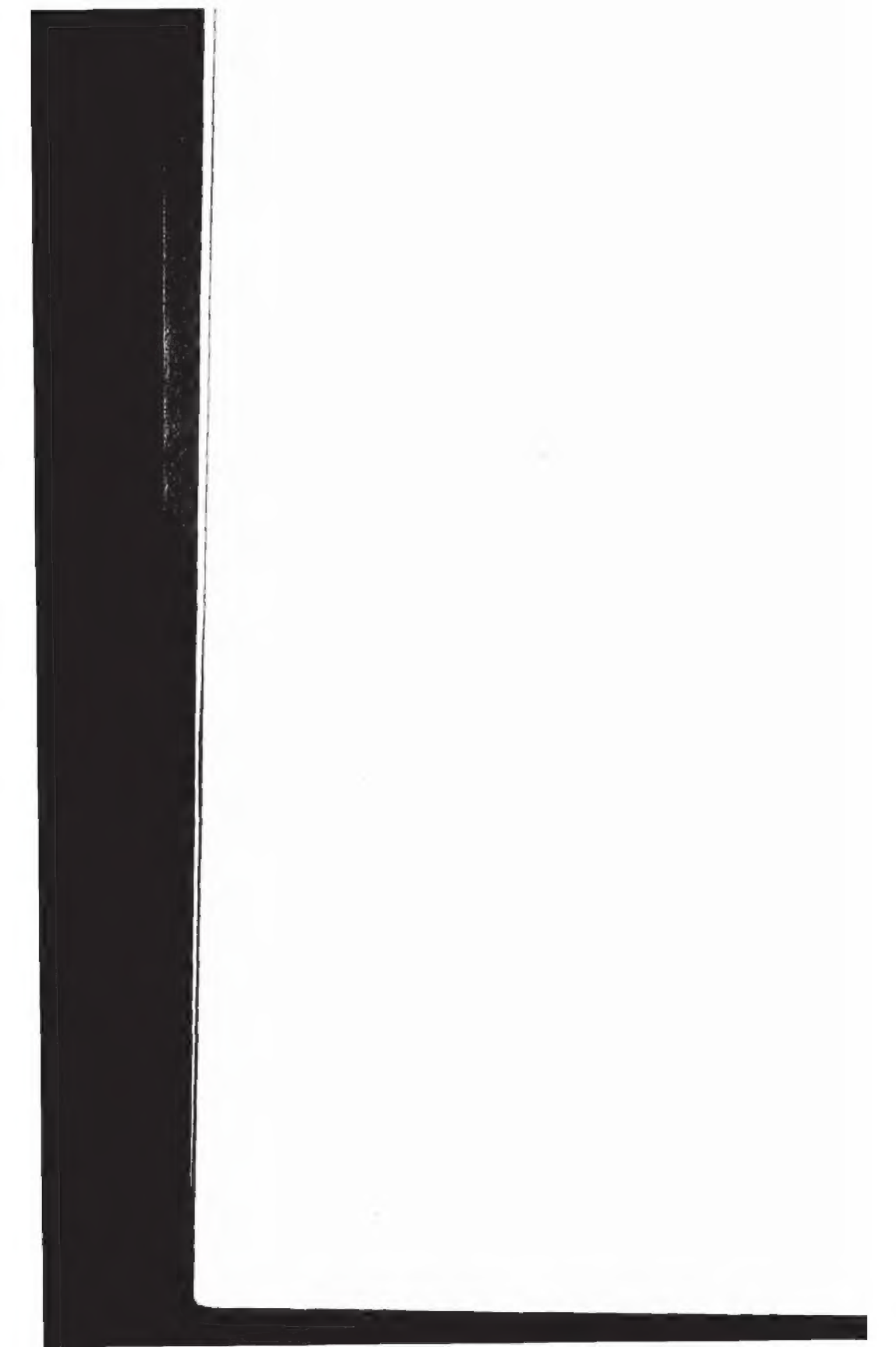
Cover design by Patrick Michael

ISBN 1-55950-072-7

Library of Congress Catalog Card Number 91-061943

Contents

Introduction	1
Part I: Tools And Techniques	
1. People Traps	9
2. Interrogation: The Basic Facts	17
3. Types Of Interrogators	29
4. The Interrogator's Mind-Set	37
5. Techniques Of Applying "Pressure"	49
6. Deceptive Tactics During Interrogation	59
7. The Covert Interrogation	69
8. Torture	75
9. The Polygraph	83
Part II: Special Applications	
10. Prisoners Of War	97
11. Pre-Employment Interviews	107
12. Media Interviews	123
13. Depositions And Court Testimony	129
Part III: Resistance	
14. Coping With Interrogations	139
15. The Language Of Lies	159
Glossary	163
For Further Reading	169
Index	173



Introduction

Life appears to be getting more complicated, and we have to cope with more pressure than our parents did. One of the types of pressure we face is the need to prevent or defend ourselves against people invading our privacy. In some cases, we have to answer questions from an interviewer or interrogator.

Many people face interrogation in one form or another during their lives. Sometimes it's during a criminal investigation. More often, an interrogation comes in a non-criminal setting, such as when applying for employment, or during a media interview.

There are techniques of obtaining information from willing and unwilling subjects, practiced each day by both skilled and unskilled interviewers. This book explains and lays out

2 ASK ME NO QUESTIONS

techniques of resistance, to help you avoid giving information or to conceal information while appearing to be cooperative.

In some cases, such as during a police investigation in the United States, you do not have to answer questions, because you're under the protection of the U.S. Constitution. However, police investigators have methods of inducing suspects to talk, despite Constitutional protection. You need to know about such techniques, which is why we'll examine these in detail.

In other situations, such as an employment interview, you're not under Constitutional protection. During employment interviews, you don't have to answer questions, but the employer doesn't have to hire you. In practical terms, that's coercion.

Your goal is to present a good picture of yourself, and conceal any derogatory information. If, for example, you once committed a crime and paid for your mistake in prison, there's no real need to reveal this to a prospective employer. Your honesty won't earn you any points, and you don't need to keep paying for your error for the rest of your life.

There are many reasons why the average person needs to defend himself. Perhaps the most important one is that the interrogator or interviewer is likely to be a pro, with much experience in his craft. He interviews people eight hours a day, forty hours a week, while most people face interviewers only occasionally. That gives the pro the edge.

Another reason is that interrogation and interviewing techniques have become very refined, and the average person needs a survival kit to protect himself. Techniques can be very subtle, designed to catch subjects off guard.

At times, you may not even know that you're being interrogated or interviewed. We'll examine how interviewers and interrogators use covert interrogations to capture damaging statements from unwilling subjects. Letting your guard down during such moments can lead to serious problems. Sometimes,

an off-the-cuff statement can be construed as an admission of guilt, and people will later recall it and interpret it in the light of your presumed guilt.

Yet another reason is that many interrogators develop a cynical and distrustful mind-set, feeling that everybody lies. Even when faced with a truthful story, they'll be seeking gaps and inconsistencies. There are also investigators who feel pressured to find a likely suspect, and are willing to shade the truth in their eagerness to please the people paying their salaries. When facing one of these, it's almost a no-win situation.

People who need help in resisting interrogation mostly are not criminals. It's not a crime to apply for employment. It's also not a crime to be employed in a workplace where drug abuse or thefts take place. There are also people caught in circumstances they didn't create.

The wife of a real or suspected defector or spy, for example, may not know anything about his activities, but will come under intensive investigation. The relative of a criminal may also face suspicion. Friends, fellow employees, or associates of people suspected of crimes also come under a cloud, and need a survival kit to help them cope.

Certain political or social organizations often come under police or FBI investigation. These are the ones to which police assign labels such as "extremist." The currently fashionable term is "terrorist," applied to everyone from right-wing groups to environmentalists. An organization's actual actions are almost unimportant, because the stigma comes with the cause.

Sometimes, simply being there is enough. In cases of employee theft, company owners and managers suspect everybody, and may employ private investigators to ferret out the guilty parties. One individual found himself suspected when his employer mistakenly concluded that there was a stock shortage. In the end, it turned out that nothing was missing, and that the

4 ASK ME NO QUESTIONS

"shortage" had been a clerical error by the boss himself. However, this employee spent a couple of uncomfortable days under suspicion.

Another example is the employee whose firm hires undercover investigators to pose as employees to ferret out employee theft or drug abuse. To the undercover operative, everyone is a potential suspect, and genuinely innocent employees will come under his scrutiny. If you're in such a situation, you'll find out how uncomfortable it can be.

It's also possible to come under investigation for activities that are perfectly legal, such as labor union participation. Although the National Labor Relations Act forbids employers to investigate or punish employees for union activity, there's actually very lax enforcement of this prohibition. In real life, employers hire private investigators to work undercover and check up on employees' union activities.

Totally innocent people who lack self-confidence, and exhibit behavior that investigators interpret as deceptive, can be falsely suspected or accused. If you, for example, have trouble maintaining eye contact with the interrogator, you're in serious trouble, no matter how innocent you may be. If you answer in a hesitant manner, this can also provoke suspicion, to an interrogator trained in the linguistic school of thought. This is why average people need special training in conducting themselves credibly during interviews and interrogations.

Often, average people do fall under criminal investigation for unintentional infractions. One simple and common example is the drunk driver who runs over and kills a child. The police certainly will question him, if they know who he is. If not, they may have a list of likely suspects, and will work at narrowing that list.

The remorseful driver may be so overcome with guilt that he runs to the police to confess, or may break down into a tearful

admission when an investigator knocks at his door. Admitting guilt won't bring the dead child back to life, and will probably harm the driver's family if he goes to prison. This is why we can make a good argument for resisting interrogation in criminal cases.

Society benefits from putting career criminals away for a long time. On the other hand, there's no benefit from ruthlessly imprisoning someone who is merely an accidental or situational offender. This can only ruin a career, tie up a prison cell and taxpayers' dollars that could see better use, and deprive the government of the taxes the person would be paying if employed.

American police officers are better than those in many countries, but they can still make mistakes. Although American officers do not willingly "frame" an innocent person just to get an arrest and clear a case, they can commit errors of judgment. In some cases, the evidence is ambiguous, and it's easy to draw the wrong conclusion. The Wylie-Hoffert murder case in New York, during the early 1960s, resulted in the police arresting the wrong man, at first, because they were under intense pressure to solve the case.

One question you might ask is whether this book will do more harm than good by falling into the wrong hands. The answer is, obviously, "no." The reason is that criminals already have this information. They know how to fool their interrogators, because they're street-smart and prison-hardened. In prison, which is really a crime university, they've taken the post-graduate course from more experienced offenders. In any event, many street criminals can't read. Organized crime figures also are adept at resisting interrogation. They have very clever attorneys, who practice deception every day, and coach their clients in the techniques.

We will cover physical torture briefly, because torture does take place in the United States, at times. We're not going to

6 ASK ME NO QUESTIONS

cover special situations, such as arrest by a foreign secret police, because most of you won't have to face such prospects. Nor will you have to endure drug interviews at the hands of CIA psychiatrists. The real hazards to average people come from average situations, such as employment and mistaken identity.

This book won't provide any magic formulas for beating interrogations. There are none. There are also no foolproof ways of extracting the truth from an unwilling or uncooperative subject. If you want to train yourself to resist interrogation, you'll have to work at it. You'll need to understand how different types of interrogations and interviews work, and memorize various tactics and countermoves. You'll have to rehearse some of your answers, and practice being interviewed. You'll have to practice before a mirror, to see yourself the way others see you.

This isn't back-breaking work, but you'll need to be serious about it. Some of it will be fun, as you see your skill improve. Most of all, the final results will be worth the effort.

Part I:
Tools And
Techniques



1

People Traps

There are several types of life situations that are traps, and people become caught in them for reasons not of their making. Some of these traps lead to interviews or interrogations.

Let's begin this study by laying out exactly what we mean by the word "trap." Obviously, a career criminal who burglarizes a house should not be very surprised if he's caught and questioned. On the other hand, someone riding in a vehicle with another person who gets stopped for a narcotics violation may be surprised, especially if he has nothing to do with the offense. It's guilt by association, one type of people trap, and falling victim to one of these traps is often merely bad luck.

There are different types. Let's look at a few hypothetical and real-life cases.

Mistaken Identity

It's possible to be caught up in innocent ways. In a city with many people, it's almost inevitable that some people will resemble each other. A crime witness may provide police with a description that fits a dozen people, and if the description fits you, police will probably stop and question you.

Police Entrapment

Police also conduct "undercover" and "pro-active" operations which sometimes roll up innocent people in the net. Some police officers go to cocktail lounges and other clubs to seek out narcotics violators. Youthful appearing undercover officers attend schools, enrolling as students. Undercover officers will even sell narcotics to arrest the buyers, according to U.S. District Judge Charles Hardy.¹ This borders on entrapment, but it happens because police are willing to skirt the edge of the law.

The problem with this sort of police work is that it tends to catch the little fish, the naive occasional or first offender, but not the hardened criminal who is street-smart and knows how to protect himself. If you, as a law-abiding citizen, attend a party during which someone brings illegal drugs, you may find yourself arrested as if you were the one who had instigated the affair. This can happen even without using drugs. Being there is enough.

Carrying A Package

Some people are asked by friends or acquaintances to carry packages for them. This is usually an innocent request, but some

people exploit their friends and acquaintances by asking them to carry illegal drugs and other contraband. If someone asks you to carry a package, especially aboard an aircraft or across a border, you should refuse unless you can see what's inside the package. However, if you trust that person, you might unwittingly end up ferrying contraband for him or her. This could happen even on a short trip across town, because some drug dealers use innocent friends to convey contraband past surveillance.

If you happen to be stopped while innocently carrying contraband, you may suffer confiscation of your vehicle, if it's in a state where the law provides for confiscation of any vehicle involved in drug trafficking. Police officers will almost certainly not accept any statement that you did not know what you were carrying. It's virtually certain that they'll interrogate you, but your answers may not help clear you.

Physical Coercion

American police officers generally don't use physical violence against those they question, as the era of the "third degree" is long gone. However, police in some foreign countries do so as a matter of course. These foreign countries are not necessarily Iron Curtain countries, or "Third World" tyrannies. In Mexico, for example, it appears to be routine. The Sonoran Bar Association placed advertisements in Sonoran newspapers, on October 27, 1989, accusing police of torturing confessions from suspects to make them admit crimes of which they were innocent.² Surprisingly, the commander of the Sonoran Federal Judicial Police defended his officers by stating that they did not beat suspects in "bad faith."

An American arrested by Mexican police officers may expect the officers to read him his "rights," but "Miranda," although a

Hispanic name, does not apply South of the border. "Rights," as we understand them, do not exist. In many countries, in fact, it's an offense merely to refuse to answer a police officer's questions. In some, physical coercion, including severe torture, is legal.

Emotional Isolation

When Edward Lee Howard, a former Central Intelligence Agency employee, defected to the Soviet Union, his wife Mary had to face questioning from the Federal Bureau of Investigation.³ Although there's no evidence to suggest that Mary, herself a former CIA employee, had defected or passed any information to the Soviets, she had driven the car when her husband had eluded FBI surveillance and escaped.

On September 21, 1985, Howard prepared to ditch FBI surveillance by having his wife drive him on a circuitous course, so that he could jump out of the car immediately after rounding a curve. He'd prepared a dummy to place in the seat, so that pursuers seeing its silhouette would not become immediately aware that he'd escaped. Although his house was under watch, the FBI agent on duty somehow missed their departure, and for several hours, Howard and his wife were out of sight of the FBI. He arranged for his wife to play a tape recording of his voice on the telephone, to deceive listeners that he was still home. It wasn't until the following evening that Howard's employer notified the FBI that Howard had left him a letter of resignation.

The net result was that the FBI did not know that Mary had helped her husband escape. Although they may have suspected her help, for all they knew he had dropped out of a rear window and scurried down a gully, the same way John Dillinger had eluded them at Little Bohemia, Wisconsin, over half a century before. FBI agents did, however, question her. They were eager

to find out if she had helped her husband in his espionage. There was some thought given to prosecuting her, but as they had no real evidence, they abandoned that idea.

At this point, Howard's wife had not actually broken the law. As Howard was not under arrest, he could not, by definition, be a fugitive. The FBI did, however, take advantage of her extreme emotional vulnerability to manipulate her. They brought in a sympathetic female agent to befriend her, and to help her cope with life without her husband. Mary, with a small son to raise, soon was cooperating, and went so far as to agree to a polygraph examination.

The FBI appeared to have milked her dry. She gave them information they could not have obtained any other way, such as the existence of a numbered Swiss bank account. She also revealed the location of a metal box containing about ten thousand dollars that Howard had buried in the desert, and went with agents who dug down and removed it. When they opened the box, they saw it contained bars of silver and assorted currency, including some South African Krugerrands.

This case is noteworthy because it shows how a single person can be made to feel isolated and vulnerable against the power of the state, and broken to the police's will, without physical torture or even severe threats. Although no detailed account of the interrogation sessions with Mary Howard are available, the main point is clear: the FBI had nothing against her, other than that she was a defector's wife. From that thin beginning, they extracted information from her by persistent and skillful interrogation, manipulating her emotions when she was most vulnerable.

Another case was that of Mike Rivera, wrongly convicted of a rape/murder in Philadelphia. According to an authoritative account of the case, police intimidated the main witness, as well as beat a confession out of the suspect.⁴ The Rivera Case shows that, indeed, it "can happen here."

Overzealous Security Staffs

At times, private security officers can suffer from excessive zeal, and try to coerce employees into admitting non-existent thefts. They may be working towards prosecution, in which case their object is to obtain a confession, or they may be seeking "restitution," in which case they try to obtain both a signed confession and money from the employee.

In one case that finished in federal court, an Eastern convenience store chain had employed security officers who coerced innocent employees into confessing to theft, under threat of prosecution, and had collected hundreds of thousands of dollars in "restitution." To date, over 300 former employees of the chain, Cumberland Farms, have become involved in a federal lawsuit against the firm, stating that they had been coerced into signing false confessions. The attorney handling the suit has estimated that the company may have coerced as many as 30,000 employees.⁵

One woman, who worked for the chain as a teen-ager, stated that her father had believed her guilty for 15 years. One divorced mother reported that when store security officers accused her of stealing \$6,000, they threatened to take her children away from her, unless she handed over \$1,500 in cash by noon on the following day. Another woman, who had admitted to taking unauthorized soft drinks while on duty, found security officers accusing her of having stolen \$2,900.

Most or all of these cases appear to have started as interrogations, with security officers taking a suspect into a back room and insisting that they confess. These people allowed themselves to be victimized because they thought that they were alone, and that nobody, including relatives, would believe them. In that regard, they had some justification, because to some

people, accusation equals guilt. Once some of the cases came to light, however, others who had been coerced into confessing began stepping forward, and some even formed a support group.

This shows the sinister side of private security. Although this is one of the few documented cases of abuse by private security officers, it illustrates the tip of the iceberg. There have been other instances of individuals falsely accused of shoplifting, for example, and coerced into signing confessions, but few have resulted in lawsuits against the abusers.

Bad Luck

You don't have to be a criminal to fall under suspicion and investigation. Circumstances can cast suspicion on totally innocent people. If you're the unlucky one, you'll need all your wits about you in order to survive. You'll also need to know the basic facts about interrogation.

Sources

1. Associated Press, November 17, 1989.
2. *Arizona Republic*, November 20, 1989.
3. *The Spy Who Got Away*, David Wise, NY, Avon Books, 1988, pp. 207-239.
4. *Notable Crime Investigations*, William Bryan Anderson, Editor, Springfield, IL, Charles C. Thomas, Publisher, 1987, pp. 315-321.
5. Associated Press, September 3, 1990.

2

**Interrogation:
The Basic Facts**

Let's begin by stating the obvious: an interview or interrogation takes place because the interviewer or interrogator needs information. If you, the reader, don't absorb anything else from this book, remember this one hard fact, because it's the foundation for everything else. In the following pages and chapters, we'll discuss many cases that highlight the same basic point.

The interrogator needs the information because he doesn't have it. He's questioning you because he hopes to get information from you. If you don't provide it, he may not be able to obtain it by other means. Sometimes, he has only part of the picture. He depends on you to fill in the rest, or to provide a lead to more information.

A skilled interviewer or interrogator's job is to persuade you to admit damaging information, or to incriminate yourself. An interviewer's manner is often bluff, to convince you that there's no point in withholding information. This works with many people, and they admit damaging facts about themselves when they could have successfully withheld them.

As a rule, people talk too much. This is true in employment interviews, criminal investigations, and various "internal" investigations that many employers conduct. In the majority of interviews, the main source of information, favorable or damaging, is the subject himself. Throughout this book, we'll be hitting at this point again and again, because it's vital. We'll discuss and study case after case in which people who could have avoided disclosing important information failed to protect themselves, and shot their mouths off to police and others. We'll also examine categories of information which are easiest to keep from interviewers.

Interviews and Interrogations

Let's distinguish between an "interview" and an "interrogation." An interview is in a non-criminal setting, or at least with someone who is not under suspicion. The subject is usually willing to speak, because he's either witness to a crime, or because he has a positive reason for speaking, such as seeking employment. The subject also may be a neighbor, relative, or friend of a suspect, or have other information which can help an investigation.

An interrogation involves a suspect or co-conspirator who may have something to conceal. A superficially cooperative attitude may mask an intent to deceive.

There's often some overlap between the two categories because the distinction between witness, victim, and suspect isn't

always clear during early stages of an investigation. An arson victim may have set the fire to collect insurance. A rape victim may be lying.¹

This is why we'll often use the terms interchangeably. The tactics are often similar, and the objectives are the same. The interviewer/interrogator tries to elicit information, and the subject/suspect either tries to avoid giving it, or tries to put across his own version of the facts.

Information vs. Evidence

In a criminal investigation, the officer who has all of the evidence he needs for a conviction doesn't need to speak with you. He's got his case, and he can convict you with absolutely no cooperation from you. If this is so, he won't be spending much time with you, but will simply throw your case into the lap of the prosecutor. This official will scrutinize the evidence, and form an opinion regarding whether or not he can easily win during a trial. Your attorney will make his own evaluation, and if he thinks he can't win an acquittal for you, will ask for an interview with the prosecutor. During this session, he'll explore the possibilities of working a deal. The prosecutor will decide how much the case is worth to him, in saving the expense and effort of a trial, and may make an offer which results in a "plea bargain." You plead "guilty" to a lesser charge, or to the same charge in return for a reduced sentence.

"Copping the plea" short-circuits the entire process. If you decide to plead guilty, the prosecutor doesn't have to present evidence, and he obtains a cheap win. Let's note here that, in reality, your actual guilt or innocence are almost irrelevant to the plea bargain. It's what the prosecutor can prove that counts, as well as your willingness to take or avoid the risk of a trial.

Most of the time, the interrogator needs a statement from you to use against you. The "Miranda" warning reads, in part: "Anything you say can be used against you in a court of law." In Great Britain, the "Judges' Rules" stipulate that the suspect receive the following warning: "Whatever you say will be taken down and may be used in evidence." This is less threatening than some fictional accounts in which British detectives warn the suspect that: "Everything you say will be used against you," but it's still enough to cause worry.

In many criminal cases, investigators don't have the physical evidence they need. Inducing the suspect to reveal where evidence is located helps assure a conviction. Many suspects don't realize how weak the investigators' case is, and they reveal details which only serve to make the case against them firmer.

Understanding The Rules

Interviewers and interrogators often employ questionable tactics, systems, and devices, such as interpreting body language (kinesic interviewing) and using the polygraph, or "lie detector." The most important fact about these systems and devices is not whether they actually work or not, but that the interviewer thinks they do. Anyone undergoing interrogation of any sort must understand these systems, and act accordingly. Anyone who ignores them will risk being branded a liar.

Do You Have to Talk?

Ernesto Miranda was a sleazy, small-time hood, arrested in Maricopa County, Arizona, in 1963 for rape and kidnaping. Miranda was not notable, in himself or in the nature of the charges against him, but his attorneys took his case to the U.S. Supreme Court, and the landmark decision that followed in

1966 bears his name. The Miranda Decision is based upon the Fifth Amendment, which protects against being forced into self-incrimination, and states that police officers must advise a suspect of his rights upon arrest, and before any interrogation. Supporting court decisions have broadened the meaning of the original ruling, so that officers cannot use information given voluntarily after an arrest but before they have read the suspect his rights.

For all that, Ernesto Miranda never changed his ways. He died from stab wounds received in a bar fight in 1976.

The Miranda Decision applies only to American police officers, but some other countries have similar safeguards for the accused. British and French police, for example, have to advise suspects of their rights, although in somewhat different language.

The Miranda Warning

The result of the Supreme Court decision was the "Miranda Warning." The exact phrasing varies somewhat with the police agency, but the substance remains the same:

You have the right to remain silent. If you give up this right, anything you say may be used against you in a court of law. You have the right to have an attorney present before questioning begins, and to be with you during questioning. If you cannot afford an attorney, one will be appointed for you free of charge. You also have the right to stop answering questions whenever you wish.

Do you understand these rights?

Do you want to give up your rights and answer my questions?

If you find an officer reading "Miranda" to you, take it very seriously. It means that criminal charges are just around the

corner. Indeed, you may already be in handcuffs when you hear the Miranda Warning. It's customary to "Mirandize" suspects when placing them under arrest.

In all cases, you may refuse to be interviewed, or to answer questions, under the protection of the Fifth Amendment, but only official police have to advise you of your rights. The reason is that the framers of the Constitution felt it was necessary to protect the citizen from the government, but not from other citizens.

This is why private investigators and security personnel do not give their suspects or detainees the Miranda Warning. With them, the questioning begins immediately, and often includes several intimidation tactics.

It's a common misconception that police officers always give Miranda Warnings. Not so. The Miranda Warning is required only in "custodial interrogation," which means when you're under arrest, and not free to leave. Preliminary investigations do not require the Miranda Warning. This is especially true if an investigator telephones you to obtain information. The dividing line is arrest. After arrest, you may not hear a Miranda Warning very often. For example, the officer who transports you to court, or to another jail, is not going to give you a Miranda Warning when he takes custody of you. He's also unlikely to interrogate you. However, if you voluntarily discuss your case with him, simply because you want to talk, and you make damaging admissions, don't be surprised if he reports your statements.

The basic decision regarding whether or not to talk depends mainly upon the answer to one question: "Who's got the power?" Related to this are the questions regarding what the questioner can do to you in reprisal if you keep silent, and what your goal might be.

In criminal cases, you simply can't turn around and walk out, because you're under physical or legal restraint. In other cases, such as an employment interview, you're free to refuse to answer

any questions, and even leave whenever you wish, but you probably sacrifice your prospect of employment if you do.

If your employer is conducting an investigation, he may insist that you cooperate. Refusal to do this is insubordination, and you face dismissal as the penalty. In such a case, your refusal will also appear to be a sign of guilt.

If you work for a law enforcement agency, you've probably already found out that you don't have the rights ordinary citizens have. If "internal affairs" officers want to question you, or put you on the polygraph, you have no right to refuse. A Pima County, Arizona, Deputy Sheriff found this out when he became involved in a fatal shooting that was later challenged. Upon discovering that he was the subject of an investigation, he consulted an attorney, who advised him not to cooperate. He refused all interviews, and lost his job as a consequence. However, he also avoided criminal charges, and is free today. As an experienced officer, he knew that a case often hangs on the suspect's statements, and correctly calculated that it would be difficult, if not impossible, to build a criminal case without his cooperation. His choice was between being unemployed and free, or unemployed and behind bars.

In yet other cases, it's not clear. If, for example, you've been accused of a questionable self-defense shooting, you may feel that you'll make your case better if you appear open and cooperative to investigating officers. On the other hand, if you're in a jurisdiction noted for its anti-gun, anti-self-defense stance, you may be better off making no statements until your lawyer arrives.

Sometimes you have nothing to lose by stonewalling an investigation. If you're guilty, but you're the only one who knows it for sure, it's foolish to make damaging admissions.

Keeping Your Mouth Shut Works

Competent defense attorneys know this, and advise their clients to keep their mouths shut. They know that an astute police officer can glean small details from a suspect's statement to lead him to tangible clues. Sharp attorneys also know that making statements to the media can be as damaging as speaking to the police.

Consider the case of John Carpenter, who has for many years been a prime suspect in the killing of actor Bob Crane. Crane, best known for his role as Colonel Hogan in the TV series *Hogan's Heroes*, was bludgeoned to death on June 29, 1978, in Scottsdale, Arizona. Scottsdale is normally a very quiet town, with few violent crimes. Therefore, the police department lacks experience in handling major cases. Police investigators had not done a very good job gathering and preserving physical evidence in the Crane killing, and they needed a confession to break the case. Carpenter's Beverly Hills attorney, Gary Fleischman, has advised Carpenter to refuse steadfastly to be interviewed by anyone, including the press, and to refer all questions and requests for statements to him. This policy has worked, at least keeping Carpenter out of jail during the years since the killing.²

Scottsdale police still suspect Carpenter, and recently failed in their efforts to obtain a DNA-typing from bloodstains found in Carpenter's rented car. Whether Carpenter actually did it doesn't matter here. The main point is that, lacking physical evidence, the only way police can obtain anything to present in court is by extracting it from the suspect directly.

Klaus Fuchs: Making Something Out of Nothing

Another case was that of Klaus Fuchs, a German Communist who fled to Britain and worked on the atom bomb project

during WWII. Fuchs had passed secret information on nuclear weapon design and development to Harry Gold, a member of the Rosenberg spy ring, and the FBI had discovered this only through the "Venona" code-breaking effort, which was super-top-secret. Both the FBI, and their British counterparts, did not want to reveal their cryptographic success against Soviet codes. This precluded presenting this evidence in court, or even revealing to Fuchs how they knew he was a spy.

British "MI-5" investigators decided to try to bluff a confession from Fuchs, assigning their best interrogator to the task. This was William Skardon, a former police officer who had joined up with the counterspies. On December 21, 1950, Skardon began a series of interviews with Fuchs, during which he induced him to believe that the government had a very solid case against him, and that it would be in his best interest to confess. Fuchs finally cracked, on January 24, 1951, making a full confession and cooperating in the effort to try to find his American contact. This was without any offer of immunity, which attests to the skill and persistence of William Skardon.³

The Fuchs case is worth studying for the lessons it teaches. The major point is that a highly skilled interrogator can bluff an intelligent suspect into a confession. Fuchs was not an illiterate street thug, but a top nuclear physicist with a life-long dedication to Communism. His interrogator, Skardon, did not work him over with a rubber hose or wet towel. He quietly and tactfully persuaded Fuchs to speak, and to make one damaging admission after another. If Fuchs had simply kept his mouth shut, the government would not have prosecuted him, because the only evidence, based on cracking Soviet codes, was too sensitive to reveal until decades after the events. The worst that could have happened to Fuchs would have been the lifting of his security clearance.

This is why, in criminal cases, the first admonition defense attorneys offer to their clients is "keep your mouth shut." They

tell them outright not to speak with police officers or anyone else about the case without their being present.⁴

Employment Interviews

Employment interviews have an important common feature with police interviews. The interviewer knows practically nothing about you, and finds out only what you list on the application form, or tell him verbally. The employment application may have a statement that you consent to a background check and understand that you may be dismissed for making false statements. However, this is usually for intimidation only, and this threat is actually illegal in some states. Employers depend very heavily on interviews and various types of tests to obtain information about their applicants. We'll explore this in depth in a later chapter.

Resisting Interrogation: Basic Tactics

If ever you're interviewed or interrogated, you'll have to make a basic decision at the outset, and stick to it. You'll have to decide whether to dig in your heels and refuse to cooperate at all, or pretend to cooperate in the hope of convincing the interrogator of your viewpoint. If you cooperate, you'll need to know the tactics of interrogation so that you may devise counter-measures. The information in this book will help you decide.

Sources

1. *Interrogation*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987, p. 4.

2. *Arizona Republic*, February 11, 1990. This news article discusses only the Carpenter case, but we find corroboration in an article by Daniel D. Evans, writing in *Law and Order*, August, 1990, pp. 90-95. Evans points out that police solve most cases, by far, through interviews, and states that officers who fail to make good cases often fail because their interrogation skills are insufficient.
3. *Mask of Treachery*, John Costello, NY, Warner Books, 1989, pp. 486-490.
4. *The Mugging*, Morton Hunt, NY, Signet Books, 1972, p. 141.



3

Types Of Interrogators

There are many types of interrogators, depending on the task and the context. Some are highly skilled professionals, while others are clowns to whom fate has given power over people's lives. The first step in calculating your chances of resisting interrogation is to understand the type of person you're facing, his level of skill, and his particular objectives.

Police Officers

These may be uniformed officers investigating crimes and taking preliminary statements, or criminal investigators who "roll out" for special incidents. For example, robberies and homicides are always cases for plainclothes investigators, and

larger police departments maintain special squads assigned to each type of crime.

Police officers handle their assignments in a routine manner, following established procedures. This doesn't mean that they're careless or stupid, but simply that they won't take any extraordinary measures to break a case. Police officers are usually as much concerned with currying favor with their superiors and avoiding lawsuits as they are with solving cases. This is not so with certain other police types.

Special Task Force Police

Today, interagency task forces are likely to be special narcotics investigation units. These task forces contain a mixture of criminal investigators and undercover officers. Task force officers are usually volunteers bored with regular police work, and who crave the excitement of unusual assignments. A feeling of eliteness pervades special task force officers, who often have special powers and are more free-wheeling than regularly assigned officers. This promotes an arrogance that is very visible, and even a feeling that they are above the law. A task force officer is more likely to plant evidence, and to rough up a subject under interrogation, than his regular counterpart.

Federal Agents

These run the gamut from Postal Inspectors and U.S. Marshals to the Federal Bureau of Investigation and the "hot dogs" of the Drug Enforcement Administration. Postal Inspectors and Marshals are low-key and competent, and noted for closing cases with minimal publicity. By contrast, the FBI and DEA agents tend to be more flamboyant, and some are outright publicity hounds.

Federal agencies share a characteristic with larger police departments: all have large budgets and resources. They can call upon officers who specialize in interrogation. They can also afford to conduct special interrogation courses for their officers, and even send officers to courses run outside their agencies.

Do Police Officers Frame Suspects?

Although there are bound to be exceptions, American police officers do not knowingly frame an innocent person. Police officers, like other workers, make mistakes, but they're usually in good faith. The reason is that police officers genuinely see themselves as the "good guys," fighting a hard battle against the "bad guys," and they try to live up to their self-image.

Police officers don't, however, always play strictly by the book. They will, in certain instances, perjure themselves to help make a case against a suspect. An example is the officer who stops a known drug dealer for a traffic offense one night. He may order the suspect out of the car, and quickly search likely hiding places, such as under the seats and the glove compartment. Without probable cause, this search is illegal, and if it turns up nothing incriminating, the officer will have to let the suspect go and stonewall any complaint. However, if the officer finds a baggie of drugs, he'll have to cover himself in court by stating that he'd seen the baggie on the seat, and deny that he'd gone fishing for it.

Finally, we have the hard-core career criminal, against whom the police have not been able to make a case stick. Some police officers will, in extreme cases, frame such a suspect. Framing consists of contriving evidence pointing towards the type of crime the person normally commits. Returning to the example of the drug dealer, a simple and common way to frame this suspect is to stop him for a traffic offense, lay a baggie on the

front seat of his car, and "find" it. For extra effect, the officer may also "find" a concealed weapon or other contraband when he conducts a full search after arresting the suspect.

Private Investigators and Security Guards

Although American police officers aren't perfect, they're pretty good compared to the human material screened out during recruitment. American police officers on every level are increasingly better-paid, and receive better fringe benefits, than they did years ago. Police agencies can, therefore, be increasingly demanding in their requirements. Those whom they reject sometimes go on to become various types of private security officers.

Rejects include various types known as "wannabes," "Ram-bos," and other unsuitable people. A "wannabe" is a person who "wants to be" a police officer, but lacks the talent or the temperament for the job. The "Rambo" type is bloodthirsty, and entirely too uncontrolled and aggressive for police duties. The person with the "make my day" mentality is simply seeking an excuse to arrest, beat, or kill someone, and is an accident waiting to happen. Another type of person unsuitable for police work is one who actually fits into a psychiatric diagnosis, such as "sociopath," "psychotic," etc. Some of these people can marginally get along in the world, but are unsuited for any responsible employment.

Private security agencies vary from excellent to simply awful. Most pay far less than police departments pay, and cannot, therefore, maintain similar recruit standards. In other words, they hire the dregs and losers as "rent-a-cops."

Private agencies are often economically marginal operations, and cannot afford proper screening procedures. Private agency owners and managers suspect, but often don't know, that the people they hire are inept, because they don't run background

checks. Instead, they rely on paper-and-pencil tests, or polygraph examinations, to screen out undesirables. This is cheap and dirty, and it shows in the results.

Military Interrogators

Captured prisoners of war are likely to face interrogation from members of their captors' military intelligence department. These interrogators vary in quality from very good to simply awful, depending both upon their organization and whom they have captured.

Military interrogators usually work under pressure to produce quick results, information useful to the battlefield commander. They may be oriented towards humane and even gentlemanly behavior, or brutal tactics, depending again upon the standards of their organizations. Another important factor is the type of prisoner and the nature of the conflict.

Some types of prisoners, such as downed airmen who have been bombing civilians, are likely to receive harsher treatment than ground soldiers fighting against other military men. This is especially true if airmen fall into the hands of civilians and civilian organizations, such as the police. Members of some paramilitary organizations, such as the Irish Republican Army, may be surprised to find their captors treating them as criminals, instead of POWs. This is partly because the Geneva Conventions do not apply to "internal security" functions, only to conflict between nations, and partly because the occupying power does not want to legitimize the insurgents by giving them POW status.

Certain cultures hold the belief that death in battle is honorable, while capture is shameful. Such soldiers are likely to treat POWs harshly, as the Japanese did in World War II. Likewise, members of some religions, such as the Muslims, feel

that their opponents in a holy war are scum, and deserve the worst they can hand out. Torture and mutilation are routine, and anyone captured by them can expect rough treatment if they refuse to answer questions.

Employers

Employers want to know who they're hiring, and therefore interview job applicants. Some interviews are fairly reasonable and straightforward, while others go off on tangents. Properly, the employer's business is whether you can do the job correctly. Everything else is none of his business. Regardless, there's still the "big brother" mentality among private authority figures, as among government officials. Some can't resist prying into other peoples' private business. We see this today in recent efforts to detect drug use among employment applicants. To the employer, it doesn't matter whether the job applicant uses drugs only on his own time. As long as he can get away with intrusion into the applicant's private life, he will.

There's also another side to this. An employer is concerned about the work history of anyone he's considering hiring. A problem personality or a dishonest employee is cause for concern.

There's a third side. There are people who have made mistakes during previous jobs, and who feel that they deserve another chance. There are others who have done things which, although not illegal, arouse resentment among many employers. One instance is union membership or activity. Potential employers often try to ferret out such behavior.

Private Parties

This includes various rare types, such as criminal gangs, political extremists, etc. Right now, the chances of a citizen's

being kidnaped and questioned by such a group are very small, but in countries such as Northern Ireland, this sort of thing happens almost every day. We also don't know what the future will bring. A social upheaval in ten or twenty years might see a new outbreak of vigilantism, and various other extra-legal actions. There would be informal and very violent interrogations, without any legal safeguards.

Attorneys

Right now, conventional wisdom states that attorneys are a scruffy lot, who earn their living by misrepresenting and even cheating their clients, or by defending people who are obviously guilty. This is a simplistic viewpoint, but there are some real-life facts underlying the negative opinions many people have of attorneys. Despite the alleged shortcomings of attorneys, many people continue to employ them.

The theory of American justice is that a trial is an adversarial proceeding, with the prosecutor and defense attorney facing off and going to the mat for their sides. Although an attorney may present the appearance of doing a forceful job of representing his clients, it's mostly for show. As Alan Dershowitz has pointed out, most defendants are guilty, and everybody knows it.

If ever you face an attorney, or need to hire one, you must understand the basic fact that your attorney's first loyalty is to the system which he serves, not to you, his client. Attorneys are members of cozy little clubs, and the prosecutor is also an attorney, as is the judge. Your attorney knows that he's best off working with the judge and prosecutor, not against them. The attorney knows that he can't afford to antagonize a judge. He also knows that "he needs the prosecutor's office and that the prosecutor's office doesn't need him."¹

Yours is only one case among many. Your attorney will have to return to face the same judge, and the same prosecutor, and he has to maintain a working relationship with them. Deep down, your attorney probably thinks you're guilty, anyway. This turns a trial into a cooperative effort, not an adversarial one.

If you hire an attorney to defend you in a criminal case, watch for one thing: Does he actually ask you if you committed the crime? If he doesn't, you can be sure that he's assumed that you did it, and that he's defending you only for the fee, or because of a belief that even guilty parties are entitled to legal defense.

In a civil case, your attorney is likely to be just as cynical, but less likely to view you as a low-life. He will take your side in court, and be with you during any deposition or hearing. Later, we'll take a brief look at what you can expect during depositions and court appearances.

What They Have in Common

Interrogators come in different uniforms, and are from different backgrounds. Whether military or civilian, American or foreign, they tend to have certain things in common. Usually, they have similar outlooks, and similar ways of treating their subjects. We'll examine these next.

Sources

1. *Discretionary Justice*, Howard Abadinsky, Springfield, IL, Charles C. Thomas, Publisher, 1984, p. 72.

4

The Interrogator's Mind-Set

Anyone facing an interview or interrogation should know that interrogators, whether professional or inept, come onto the scene with certain assumptions and mind-sets. Although they make a serious effort to present themselves as "objective," they're really not objective at all. It's important to know the unspoken ground rules, and understand the hidden agenda.

Attitude

Many interrogators adopt distinctive attitudes, which determine their tactics. Recognizing these attitudes can provide clues as to the tactics to expect.

Everybody's Guilty

This is the extremely cynical viewpoint that affects many police officers and private investigators. They encounter so many suspects, and see so many skeletons popping out of closets, that they feel that everyone has committed some sort of crime during his life. It's easy to move from this feeling to one that suspicion equals guilt, and that suspects acquitted in court go free simply because police and prosecutors failed to find enough evidence to present, not because they were actually innocent.

Everybody Lies

This is the corollary to "everybody's guilty." If they're not guilty of a particular offense, they're still lying about their role in the matter, because they have something else to hide.

This is also true of people who conduct employment interviews. Some feel that at least half of their interviewees exaggerate their qualifications and experience, and cover up damaging information. One serious study found that 30% of the resumes they surveyed contained "outright lies."¹ Thus the question is not whether the subject has any faults or shortcomings, but whether the interviewer can reveal them.

Get, Don't Give

This is a standard technique used by police and other interrogators. The purpose is to reveal as little information as possible to the person being questioned, yet try to get as much as possible from him.² To this end, the interrogator carefully conceals what he already knows, and will even tell the subject a lie to induce him to cooperate.

One example is the questioning of a suspect's parents by a detective assigned to the Clutter murder case, popularized in the

book, *In Cold Blood*, by Truman Capote. Harold Nye, the detective, interviewed the parents of one suspect, allowing them to think he was interested in their son only for fraud and parole violation. He felt that, if he'd told them he was working on a murder case, they would have been less forthcoming.³

Nye was cautious, but he'd already made an error that, luckily, had not compromised the investigation. He'd traveled to Las Vegas to interview the former landlady of one of the suspects, and told her that he was investigating a parole violation. She expressed disbelief that he'd come all the way from Kansas for such a petty matter, but answered his questions anyway.⁴

Having learned from this, Nye used a different tactic when he traveled to San Francisco to interview the sister of one of the suspects. Nye told her that he was "attached" to the San Francisco police, and was responding to an inquiry from officers in Kansas who were trying to locate her brother, who hadn't been reporting to his parole officer. To avoid alarming her, he didn't mention that he himself had traveled all the way from Kansas, and he never mentioned the murder investigation.⁵

Another facet of interrogation following this principle is that a successful interrogation has the interrogator contributing about 5%, and the suspect 95%. The point is to ask open-ended questions, forcing the person to provide more information.

An incompetent interrogator asks the suspect questions that he can answer with a "yes" or "no," such as: "Did you do it?," "Did you have a gun?," etc. He does most of the work, and the suspect simply denies everything.

Criminal Types

Certain classes and certain minorities are, in the eyes of the police, more likely to be suspects than others. This is because national crime statistics show that, in proportion to their numbers in the American population, they commit more crimes.

Blacks, for example, commit a greater proportion of the violent crimes.⁶ This leads police officers, who prefer to follow the main trends, to suspect members of groups often involved in crime.

Police also see certain types of people as "riff-raff," and the most likely suspects when a crime comes down.⁷ A criminal record, in their view, predisposes to more crime. They also feel that many people with criminal records have committed more crimes than those with which they were officially charged.⁸

There's some justification for this belief. The clearance rate for burglaries, for example, is at an all-time low, 14%, and this includes only burglaries reported to the police.⁹ According to another recent study, victims reported only 49% of burglaries to the police.¹⁰ These figures make the bottom line very clear: Most criminals get away with many of their crimes.

This is yet more justification for the belief that suspects are lying when they're denying. A sidelight to this is the subject caught in a lie.

One Lie Makes The Entire Statement Suspect

This is a common assumption among police and private investigators, and employment interviewers. If they catch the person in a single untruth, they assume that the person's covering up, and they discount his entire statement.

Some cynical interrogators use this to apply pressure to their subjects, by asking so many questions, about so many topics, that the subject's bound to make a mistake on one or more details. The interrogator then uses this contradiction as a lever to pry the "truth" from the subject, and to impel him to speak and reveal more information.

Evasions Are Incriminating

A reply that doesn't answer the question directly is an evasion, in the interrogator's eyes. Saying: "I don't remember" can be construed as an evasion.

One system of linguistic analysis applicable to suspects' statements holds that, unless the subject provides a clear-cut answer, he did not answer the question. Furthermore, if he does not answer the question, he actually does, in the inference the interrogator can draw from the evasion.

I'm Smarter Than He Is

Many types of interrogators have tremendous egos. They feel that, because of their intellect or their positions, they are superior to the people they question. At times, this superiority depends upon their using little conversational tricks, such as loaded questions, or simply on their power to approve or deny an application for employment.

All successful interrogators are fairly skilled actors. They feign surprise, suspicion, anger, and other emotions as manipulative tools to use on their subjects, while remaining in control of their emotions. At times, a raised eyebrow is more effective than an outright statement of disbelief, because it requires no explanation and no justification.

Enough's Enough

Some interrogators will adopt a business-like, almost abrupt manner, brushing aside any denials, and insisting upon a confession. Although they won't say it in so many words, they project an attitude of: "Yeah, yeah, I know all that. Now let's get to the truth." They refuse to get involved in a discussion of alibis or denials, as if these are simply a waste of time.

One such interrogator was William W. Barnes, an investigator with the New York State Police. According to his colleagues, he had an uncanny skill of tuning in to the mind-set of his suspects, and quickly finding the key to their personalities, which he would use to make them talk.¹¹

Barnes was the interrogator who cracked Marybeth Tinning, who allegedly murdered all but one of her nine children. Almost incredibly, this woman had had child after child die young, and although there were whispers and suspicions, there were no investigations, and no criminal charges, until after the death of her ninth child. Surprisingly, all deaths occurred in the same area, the city of Schenectady, New York, and its suburbs, and many people who knew Tinning knew of at least several deaths of her children. During the investigation of the ninth death, exhumations of previous dead children were unsuccessful because of extensive decomposition. This, and the lack of any direct evidence, made the case against her circumstantial. In fact, her attorney felt that, apart from her confession, "the prosecution wouldn't have a case."¹² Police strategists therefore made a supreme effort to bulldoze Tinning into a confession before she had a chance to think over her situation, and realize that she needed an attorney.

Barnes sat down with her, after she'd been questioned by other investigators, and adopted a sympathetic manner. He quietly insisted that she tell him the truth, asking her at one point, "How many more children have to die?"¹³ Tinning quickly admitted her guilt, and over the next few hours, provided details to flesh out her account and make it believable to a jury.

Body Language

Many investigators believe that body language provides clues to personality, guilt or innocence, and truthfulness. This is a

trendy topic, and many police investigators attend schools that teach "kinesic" interrogation. The theory is that certain poses and gestures indicate that a subject is deceptive. Some of the poses and gestures that allegedly betray a liar are holding the chin on the chest, breaking eye contact, blinking, looking at the ceiling, and dilated pupils. Smiling is also allegedly indicative of lying, as is holding the shoulders slumped. Holding the elbows close in to the body, covering the eyes with the hands, rubbing the nose, holding arms crossed, and clasping the hands in front of the body are also alleged indicators of deception. Crossing the legs or moving the feet beneath the chair are also signs of deception, according to this theory.¹⁴

The importance of this body language is not that it's an accurate indicator of deception, but that an interrogator thinks it is. A nervous or timid subject who exhibits such body language will make a negative impression on an interrogator, while a practiced liar, such as one who earns his living selling used cars, can assume a confident manner, avoid making the "wrong" gestures, and appear truthful.

Payback

This is one of the least documented aspects of police and investigatory work, but it affects investigators' attitudes almost every day. A basic rule is that of reprisal, known to police officers as "payback" or "catch-up." If, for example, a suspect resists arrest, and injures the officer, the officer will be tempted to injure him at least as much, if he can get away with it. This may happen at the site of the arrest, or in the local jail, where the suspect takes an unscheduled trip down the stairs, head-first.

Needlessly antagonizing a police officer, or even a private investigator, is a serious tactical mistake. The investigator views himself as merely doing his job, earning a living and performing

a useful social function. He takes a philosophical attitude, even when he fails to make a conviction: "You win some, you lose some." To him, one suspect is much like another, unless he stands out for a special reason. Some ways in which suspects earn unwanted extra attention are:

Showing an arrogant attitude.

Making personal remarks or insulting the investigator.

Threatening him or his family.

Any physical assault.

Any of these turn the case into a personal one. The investigator will put in extra work to secure evidence and obtain a conviction. Some might even manufacture evidence. Even with a total acquittal on the charge, the suspect will face close scrutiny in the future, and be a subject of special investigation. In practical terms, this means an investigator will seek out additional violations, even petty ones, simply for harassment. It can also mean extra attention from other departments or agencies, such as the narcotics bureau, or the Internal Revenue Service.

Ego Involvement

To an investigator, a case is a challenge to his competence, and to his ego. This is good, in the sense that it provides motivation for doing a good job. The other side is that an investigator who becomes too ego-involved loses his perspective. Some go to the extreme of seeking a confession at any price. The result is the invitation to a plea in a criminal case. The investigator bulldozes the suspect, telling him harshly that if he confesses, he'll get a reduced sentence, while if he holds out and pleads innocent, the judge will throw the book at him.

When the investigator gets to this stage, he's lost all objectivity, and doesn't care whether his suspect is actually guilty or not. The dangerous aspect of this process, as far as the suspect is concerned, is that the criminal justice system doesn't care, either. All that counts is the numbers. The prosecutor seeking a high conviction rate may offer deep "discounts" to those who make his life easier and plead guilty. The overworked judge also has an interest in seeking quick dispositions of his cases. The public defender, if you can't afford a private lawyer, is also interested in pleading his client and moving on to another case. If you're caught in such a situation, you'll be dismayed to find that nobody cares whether you're guilty or not, because you're just another obstacle they have to overcome.

Mind-set and Its Dangers

As we've seen in this chapter, and will continue to note throughout the rest of the book, interviewers and interrogators often have an unshakable faith in their particular "system," whether it be the polygraph, linguistics, or kinesic interviewing. Whatever the system, its practitioners will tell you honestly that they've found that it works. With further probing, you may obtain an admission that the technique works most of the time, but not always. Some will even candidly cite a percentage of success, which by simple subtraction, provides a percentage of failure.

The problem comes when interrogators forget that their systems have their faults, and act as if their particular technique were infallible. Compounding this problem is the overlap between systems, so that many interviewers and interrogators are eclectic, borrowing from several different techniques. This appears pragmatic, but carries a hidden danger.

An interviewer who chooses to disbelieve his subject can find many reasons for concluding that the subject is deceptive. He may note that the subject appears nervous, and interpret that as a sign of guilt. If the subject denies guilt outright, he can dismiss this as a lie, on the basis that most are guilty, anyway. This is especially true if the subject is a minority group member. If the subject hedges his answers, the interrogator can take the linguistic approach, and conclude that, as the subject isn't answering the question directly, he's a suspect. He can also interpret a misstatement as a deliberate lie, and reject all of the subject's denials, no matter how forceful and direct they might be. One authority even states that repeated assertions of innocence are themselves incriminating.¹⁵

The other side of mind-set is that it blinds the interviewer or interrogator to the ones who get away with deception. The many successes are usually with people who are naive, suggestible, who lack "street smarts," and who are not career criminals. Those who succeed in deception are those who work at it, such as used car salesmen, lawyers, professional con artists, and other career criminals. These experienced deceivers are not going to fold up and tell all when faced with a polygraph test, nor will they let themselves be duped by an interrogator's bluff.

Understanding Mind-set

When facing interrogation, most subjects arrive unprepared. A competent interviewer or interrogator makes an effort to know and understand his subject. The reverse is rarely true, which is one reason why many people fail to do well under interrogation. The pro tries very hard to "read" his subject or suspect, while the naive subject simply waits for the interviewer to make his moves. Knowing how interrogators and interviewers think, and understanding their mind-sets and motivations, is a vital basic step to resistance.

Sources

1. *The Book of Lies*, M. Hirsch Goldberg, NY, William Morrow and Co., 1990, p. 15.
2. *Notable Crime Investigations*, William Bryan Anderson, Editor, Springfield, IL, Charles C. Thomas, Publisher, 1987, pp. 67-68.
3. *Ibid.*, p. 16.
4. *Ibid.*, p. 20.
5. *Ibid.*, p. 23.
6. *Criminal Victimization in the United States*, 1986, Washington, DC, U.S. Department of Justice, Bureau of Justice Statistics, p. 44. According to this criminal victimization survey, 24% of single-offender violent crimes were committed by black offenders, according to victims. Blacks do not comprise 24% of the U.S. population, but only about half that percentage. In multiple-offender crimes, cited on p. 49, the proportion is even higher; 32.4% all black, and 9.4% with offenders of mixed races.
7. *Notable Crime Investigations*, p. 314.
8. *Ibid.*, p. 325.
9. *Use of Forensic Evidence by the Police and Courts*, Joseph L. Peterson, Washington, DC, National Institute of Justice, U.S. Department of Justice, Research in Brief, October, 1987, p. 1.
10. *Reporting Crimes to the Police*, Catherine Wolf Harlow, Ph. D., Bureau of Justice Statistics Special Report, Washington, DC, U.S. Department of Justice, December, 1985, p. 2.

11. *From Cradle to Grave*, Joyce Egginton, NY, William Morrow and Company, 1989, p. 214.
12. *Ibid.*, p. 251.
13. *Ibid.*, p. 219.
14. *Law and Order*, August, 1990, pp. 90-95.
15. *Lie Detection Manual*, Dr. Harold Feldman, Belleville, NJ, Law Enforcement Associates, 1982, p. 181.

5

Techniques Of Applying "Pressure"

The first task for the interrogator is persuading the subject to speak, because without active cooperation, there can be no progress for the interrogator. Police agents and other interrogators have various ways of inducing subjects to talk. Some are simple rapport and conditioning techniques, and we'll begin with these.

Rapport

Establishing "rapport" to lull the subject is the beginning. Most people come to interviews and interrogations apprehensive, and remain on their guard throughout. One way of defusing the situation is to work hard on presenting a pleasant manner

with the subject. This begins with courtesy, and continues with accepting without question everything the subject has to say.

The interviewer trying to develop "rapport" will often engage in small talk designed to show the subject that he and the interviewer have something in common. There may even be a display of feigned sympathy for the subject.

The purpose is to develop "rapport" with the subject, and it doesn't always work. Rapport is always limited because the obvious fact is that the interviewer or interrogator is not your friend! The best that the interrogator can hope for is a cautious but polite exchange, unless you fall for the phony friendliness.

Conditioning

Conditioning the subject to answer questions is a technique that applies to all interrogations and interviews. Setting up rapport and conditioning work together to persuade the subject to "open up" and answer questions. The interrogator begins with routine, non-damaging information, such as asking the subject his name, address, telephone number, and other basic details. You can easily get taken in by this technique, because you see no harm in telling the interviewer what he already knows.

Conditioning is a powerful technique, and the interrogator will really fight to get you to accept it. If you tell him that he already has this information on file, his stock answer will be that he is simply trying to verify his information.

There's a second purpose behind asking routine questions. This is to establish a "baseline" of behavior as he notes your reactions to questions. He'll be watching your eyes, your expression, your posture, and other body language as he takes you through routine matters. Later, when the critical questions come, he'll watch for behavior changes, which according to theory

denote stress. Fidgeting and changes of posture supposedly betray areas of special sensitivity.

Another aspect of conditioning is creating the expectation that the interrogator has the power to gratify or frustrate the subject. In criminal settings, an early step is to confiscate cigarettes, chewing gum, etc., and to dole them out to the subject. Satisfying hunger, thirst, and other physical needs also depends on the interrogator's consent. The purpose of these apparently petty tactics is to demonstrate that the interrogator has power over the subject.

Intimidation

Other interrogators begin with a harder line. One technique of intimidation is for the interrogator to be seated at a desk when you enter the room. He reads a file, occasionally looking up at you with a scowl. A variation on this theme is for the person who brings you in to hand the interrogator the file, and to stand by while he reads it. This is designed to suggest that the file is about you, that it contains a lot of information, and to give you time to worry over how much the interrogator knows. It's a serious error for you to assume that the file contains anything worthwhile.

At times, the interrogator is physically much larger than the subject. This, coupled with an angry manner, can cow a subject.¹

A very crude, but forceful, intimidation technique is to play tape recordings of people screaming outside the interrogation room. This suggests that torture will follow if no cooperation is forthcoming.

The "good guy-bad guy" technique is old, but still works. One interrogator is hard and uncompromising, while the other is gentle and sympathetic. They take turns working on you,

depending on the emotional relief you experience when the bad guy leaves the room to persuade you to speak with the good guy.

Repetition and Fatigue

Your statements provide three important possibilities to the interrogator. First is the prospect of an admission of guilt. The second prospect is providing him information he did not have before, some of which may be "leads," or avenues of further investigation. The third, and most subtle, is errors or evasions, which he can turn against you as "proof" of your guilt. Pounding away at errors and inconsistencies as signs of evasiveness can be intimidating, which is why some interrogations are lengthy.

An interrogator can wear you down by continuing the session, going over the same ground again and again. One purpose is to force you to make mistakes. Interrogators do this by insisting upon answers, even when you're not sure. You probably cannot tell the same story many times without introducing a few contradictions. Endless questioning will tire you, and phrasing the questions differently can bring forth different answers. The interrogator then uses these inconsistencies to accuse you of lying, or evasiveness.

Verbal Tricks

There are several intellectually and emotionally dishonest ploys many interrogators use to take advantage of a subject's vulnerabilities.

"I just need you to answer a few routine questions."

This approach is an effort to get you off-guard by pretending that the interrogation isn't important, but "just routine." If you

relax, and speak without thinking, you may give away something important.

You can expect the interrogator to begin with innocuous questions, such as your full name, your address, and place of employment. This is both to round out his information about you, and to condition you to answering his questions.

"I'm only trying to help you."

This statement pretends sympathy for you, and for your situation. It's transparently false, as any police interrogator truly trying to help you would remove your handcuffs, open the door, and let you walk out.

"I want to give you a chance to tell your side of the story."

This is a bluff often used by both police and media interviewers. It suggests that someone else has already made statements, or presented evidence, which disparages or incriminates you. The seemingly generous offer to allow you to present "your side" is only a ploy to get you to talk, in the hope that you'll provide more information which they can use to build a story or case.

If you want to expose this line of approach for its falsity, ask the interrogator outright: "Who said it about me, and what did he say?"

"What are you trying to hide?"

This question contains a presumption of guilt. Anyone faced with this, or a similar question, should come right out and accuse the interrogator of asking a loaded question. Another way is to answer the question with a question: "What are you trying to make me say?"

"If you're innocent, you shouldn't mind answering a few questions."

This flat statement is a contradiction of our American Constitution's Fifth Amendment regarding self-incrimination. The interrogator is telling you that your silence is proof of your guilt. You answer it by stating flatly that it's because you're innocent that you're not going to stick your head in the noose.

"You want to see the guilty person caught, don't you?"

This reflexive question is another conversational trap. It is designed to put you in the awkward position of having to answer "yes" or admit that you don't want to see justice done. The way to handle this one is to reply that if the interrogator wanted to catch the guilty person, he wouldn't be interrogating an innocent person such as yourself.

"Please answer my questions, so we can all go home."

Implicit in this statement is the promise to release you if you answer his questions. Don't believe it for a moment.

"You'll feel better if you talk to me."

This promise of emotional relief is a gut-level effort, using suggestion. The interrogator promises an end to the unpleasant emotions you're feeling, in return for your answers, but he doesn't necessarily explain why incriminating yourself will make you feel better. Surprisingly, this suggestion works with some people. If faced with this statement, simply reply that your conscience is clear.

"You lied before. Why should I believe you now?"

This is a technique of bullying used when you've made an error, or even lied, and he's caught you. It's almost inevitable,

if the interrogation lasts for many hours. The best reply is a simple denial that you've lied.

Squeezing More Information From You

Interrogators and interviewers have a repertoire of techniques and conversational tricks to get you to say more than you'd planned. Some are simple verbal ploys, based on suggestion. Others are intellectually dishonest, such as "loaded" or "leading" questions.

A basic technique is to say "and?" whenever you stop speaking. This suggests that there's more to tell. If you are suggestible, you can be spilling a lot of information under a barrage of "ands." The best response is to say simply: "That's it."

A variant on this theme is for the interviewer to say: "Now tell me the rest." You answer: "I already have."

The "predicated question" is one often used by psychologists, employment interviewers, and others who can't impose legal sanctions to pry information from you. This type of question carries an unstated assumption that you have already done something. A typical predicated question would be: "How old were you when you began to masturbate?" Another is: "Tell me about the last time you were fired."

Some are just word games, and a fairly intelligent suspect may see through them. One example is the double-bind suggestion, "Would you like to tell me about it now, or in ten minutes?" A good answer to that trick question is: "I've already told you all there is."

The single-word question is a technique used to obtain information without indicating which way the interrogator expects the answer to go. For example, he might ask you: "Where did you go yesterday?" Your answer is: "To see my

friend." His one-word question would then be: "Friend?" And he'd follow this by simply staring at you, as if expecting an answer. This is an extremely economical technique of eliciting information from those who are vulnerable.

The way to reply to this is to simply repeat the word, in a positive tone: "Yes, friend." Another way is simply to nod "yes" as if to confirm that that is what you said.

Private Investigators and Employers

As we've seen, private investigators don't have to provide a "Miranda" warning. Lacking official police powers, they also are not under the same restraints. Private investigators tend to be far more deceptive than official police. Employers are free to be more coercive. The threat of firing is a real one, and an employer can make it stick.

Of course, he cannot fire you for having committed a crime unless he has proof that you did. If he tries, you can sue him and win, but he has other grounds which make this unnecessary. He can simply order you to cooperate in the investigation, and if you refuse, fire you for insubordination.

Once you agree to cooperate, you may expect a private investigator to hammer away at you, pushing hard for information. If it becomes apparent that you're innocent, he may shift his main line of questioning to asking you who you think might be guilty. Parallel lines of questioning will cover which fellow employees use alcohol, drugs, and which gamble. Another angle is to ask you which employees you like, and which you dislike. This gives the investigator leads regarding who would be more likely to provide disparaging information about you. It also opens up opportunities to obtain disparaging information about other employees from you.

Beyond Pressure

Interrogators and interviewers begin with mild pressure, expecting to obtain compliance and answers to their questions. Some subjects are resistant, and they have an array of deceptive tactics to employ in prying information and admissions from them. We'll study these next.

Sources

1. *The Mugging*, Morton Hunt, NY, Signet Books, 1972, p. 97.

6

**Deceptive Tactics
During Interrogation**

As we've seen, many interviewers hold the attitude that their subjects are an inferior class of people, and this leads them to feel that these people therefore deserve no consideration. This is especially true of police interrogators. They have to work within the limitations of the "Miranda" decision, and a series of court decisions banning torture and the "third degree." Now that force is out, deception is in.

Other types of necessity also dictate tactics. In certain types of cases, there's no real evidence pointing to a single suspect, and solving the case depends on a skillful interrogator's narrowing the suspect list.

Let's consider industrial espionage. A bank or credit card agency may have discovered a "leak," with an employee passing

authorization numbers or other confidential information to a fraud ring. The only evidence of this is a rash of unauthorized withdrawals at automatic teller machines in the area. Security officers feel that one or more employees with access to the information may have passed it to unauthorized persons. This puts everybody on the spot. In the investigators' minds, everyone's potentially guilty until proven innocent, and the only way to find out who did it is to obtain a confession. As in the Klaus Fuchs case, the only tool available is bluff.

In other cases, investigation and interrogation are merely fishing expeditions. Members of certain unpopular organizations have found themselves being investigated and interrogated by FBI agents because they did not know that they had the right to refuse to answer questions.¹

Bluff

Many deceptive tactics depend on bluff. The interrogator is both an actor and a salesman, and his job is to sell the subject the idea that he should confess. He can do this by selling him the idea that the interrogator already knows the truth, or that he has evidence which points to the subject's guilt. Let's look at the many forms of bluff.

"We already know everything, so you may as well confess."

This is one of the oldest tricks in the book, but it can work on people who are not too bright. If you have anything better than a room-temperature I.Q., your reply should be: "If you already know everything, you don't need any more information from me."

"Your partner's already told us everything."

This can be devastating if true, and a crude lie if not. The best answer is to tell your interrogator that you're not surprised, because your partner would say anything to get off the hook. You then repeat that you're innocent.

Stating that the partner has already confessed is a standard tactic, recommended by experts in criminal investigation.² It works because many suspects know how sleazy their companions are, and feel that their "friends" would throw them over for personal advantage.

"We've already got the evidence."

Stating that they already have evidence to convict him is another deception police use to soften up a suspect. Some interrogators will even stage a fake line-up to arrange for an "identification" by someone posing as a witness. In extreme cases, they'll even accuse you of other, more serious crimes, to induce you to confess to the "real" one to get yourself off the hook.³

"Is there any reason someone would say they saw you there?"

This is not an outright lie, but is deceptive nevertheless. It's an insinuation, a suggestion that someone saw you at a certain place, without actually saying so.⁴

The only way to handle this is to answer "no." Trying to elaborate can drag you into a swampland of discussion regarding where you actually were, and lay the way open for more deceptive tactics. A simple "no" answer tells the interrogator that he can't get a rise out of you by a shocking disclosure, true or false.

"They just identified you."

Some police investigators will conduct a faked line-up, with someone playing the role of witness to point out the suspect as the perpetrator.⁵ This is outright deception, but it's allowable because there are no court decisions banning police officers from lying to suspects. They may bluff as much as they wish.

The lie may take the form of a question similar to one mentioned above: "What would you say if we told you a witness said he saw you?" One answer to that is: "Tell it to me and see." Another is: "Show me the signed statement and maybe I'll be able to give you an answer." In both cases, you're politely calling the bluff.

"Give Them Enough Rope."

A skilled interrogator will allow his subject to tell his entire story, without showing any disbelief, the first time around. He patiently records everything the subject says, and if he spots a discrepancy, he makes a mental note but says nothing until the end of the statement. This is the deception, intended to lull his subject, and fool him into thinking that he can slip any lie past his questioner.

"This is your last chance."

Some interrogators try to gain the suspect's cooperation by stating that they have been in touch with the prosecutor, and that the suspect has an opportunity to work a "deal," *if he acts now*.⁶ This is a variation of the advertising theme of "Limited time only," and is just a way to make the suspect feel a sense of urgency. In fact, such an offer holds absolutely no water unless the prosecutor signs a written agreement, preferably with your attorney present.

The Post-test Interview

As we'll see in the chapter on the polygraph, a question-and-answer session after the test itself is often productive. Although most subjects who are going to admit deception do so before they undergo polygraph testing, some resist until afterwards. At that time, the polygraph technician tells the subject that he's having a "problem" with one or more answers, and asks whether or not the subject can tell him something more that will clear up the question.

Sometimes, this takes the form of a vague accusation that the subject hasn't told all he knows. This often happens after a written statement subjected to linguistic examination. The subject may get another questionnaire, stating that the investigator has determined that he hasn't revealed all important information, and asking him to explain this. This isn't a very strong accusation, and is designed merely to make the subject uncomfortable enough to be more forthcoming.

The same thing can happen with "honesty" questionnaires. The interviewer can state that the answers show that there is a "problem" with the subject's drinking, relations with a former employer, etc., and ask for clarification.

There are two ways to handle this sort of post-test interrogation. The first is simply to deny that there's anything more to tell. The interviewer's statement is vague enough to be meaningless, and he's not going to be able to push the issue very far.

The other way is to feign a cooperative attitude, and say something like:

"I'd like to help you. Perhaps if you could be more specific, it might jog my memory and I'd be able to help you out."

This calls his bluff immediately, and usually stifles any comeback. The word "perhaps" avoids committing you to answering.

The Faked Ending

In non-criminal settings, deception often plays a major role. This is because coercion is not as strong, and the interviewer has to attain by guile what is denied to him by force.

A clever interviewer will often try to put the subject off guard by cueing him that the interview is "over." The purpose is to make him relax, and be less guarded in his statements. Anyone taking part in any interview, for any purpose, should be aware of these tricks, because no law can protect him against them.

One trick is to put down the pen, close the notebook, or turn off the tape recorder. The interviewer leans back, to give the impression that the session is over. This is when the interviewee should increase his alertness, because the real interview is only beginning.

There are variations on this. The interviewer may suggest taking a break. If it's lunch-time, he may suggest going out to eat, and make what passes for small talk during lunch. This is when you should be the most careful. If alcohol is available, you may have a drink, but only if the interviewer orders one for himself. If he asks you to order first, play it safe and decline the drink. Don't say that you never drink, unless you belong to a religious group that forbids drinking, or you don't drink for medical reasons. Instead, say that you have to drive, which is the currently trendy answer. This lets you off the hook even if the interviewer orders a drink himself, and forestalls the suspicion that you're an alcoholic frantically trying to deny it.

Over lunch, the interviewer may ask you some leading or loaded questions. Before answering, you have to think about his question on two different levels. First, you have to provide an

answer to the question. You must also think about what he's really after with each question.

The informal questioning may start with his offering you a cigarette. You may answer that you don't smoke, which is the safe answer these days, as some companies have policies against hiring smokers. He then may mention that one of his neighbors or friends uses cocaine, and make some positive statements about this neighbor.

WATCH OUT! This is the come-on. He's implying that he approves of cocaine use, just to try to pry an admission from you. If he asks you directly if you use cocaine, just say "no." If instead he sits and stares at you, as if expecting an answer, you can say that someone you knew in college did. If he follows up with a question regarding how many of your friends use cocaine, or other illegal drugs, you can simply say "None. I don't hang around with that sort of crowd."

This is the safe answer, in Salt Lake City and most other parts of the country. In certain locales, such as Southern California and New York City, it's almost incredible that someone could reside there without having many acquaintances and neighbors who use drugs.

Another question may relate to alcohol use. If he asks you what you like to drink, you can answer that you like beer or wine with a meal. This is a safe answer, except in Salt Lake City. If your prospective employer finds any alcohol use intolerable, you have to consider whether you'd feel comfortable working for such a person.

Discussing politics is like walking blindfolded through a mine-field. Be especially careful, and listen carefully to cues regarding his political beliefs. You may not be able to out-guess him unless you already know about him or his politics. Also keep in mind that he may throw out some radical ideas just to test you. The general rule is that employers aren't seeking extremists. Don't express any sympathy with the Socialist Worker's Party, the

Order, or any way-out group, unless you know for certain that your prospective employer is a member. A simple answer is to say you've never heard of the group, and that politics doesn't interest you very much.

Watch out for questions about art and literature. An interviewer may ask you if you've read any of Gore Vidal's novels, on the theory that anyone who enjoys Vidal's work must be homosexual. Likewise with authors such as Arthur Miller and Ayn Rand, who are strongly political. Miller is strongly leftist, while Rand is right-wing. Reading their works may appear to imply that you share their politics.

You might also find the interviewer bringing up other current and controversial topics, such as gun control, capital punishment, abortion, etc. These are hard to deal with directly, except for one vital point. Never, but never, get into an argument with a potential employer over politics or anything else. The purpose behind bringing up controversial subjects may well be to try to get a "rise" out of you, and to see if you're the contentious type. Businessmen seek employees who fit in, and who are team players. This means people who get along with others, not people who get into arguments easily.⁷

If an interviewer asks your viewpoint about a controversial topic, state it briefly, then shut up, especially if he contradicts you. A simple way of closing a discussion, without actually conceding, is the simple statement: "You may be right."

Remain Alert

From this section, it's easy to see that some interrogators and interviewers can be very tricky. Some will try to make up with deception what they lack in interviewing skill. This is why it's smart to remain alert and aware, from the start of an interview until you're actually out of the interviewer's presence.

Deceptive tactics don't end with the interview or interrogation. Some interrogators are extremely sneaky, and attempt to pry information from people without telling them that they're being interrogated. We'll study covert interrogation next.

Sources

1. *War At Home*, Brian Glick, Boston, MA, South End Press, 1989, p. 53.
2. *The Mugging*, Morton Hunt, NY, Signet Books, 1972, p. 107.
3. *Ibid.*, p. 107.
4. *Law and Order*, August, 1990, p. 92.
5. *The Mugging*, p. 105.
6. *Law and Order*, August, 1990, p. 93.
7. *Interrogation*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987, p. 220.

1. The first part of the document is a list of names and titles, including "The Hon. Mr. Justice" and "The Hon. Mr. Justice".

7

**The Covert
Interrogation**

There are several types of covert interrogations. Some depend upon a person who does not appear to be an interrogator teasing information from the subject while he's unaware that he's being questioned.

Pre-employment Traps

One is the fake employment candidate. During interviews, candidates wait in an anteroom to be called. One returns from his "interview," sits down next to another, and says: "Boy, that was rough! They asked me if I used drugs. I didn't admit anything. Are you going to tell them?"

Police Informers

This is a variation of the fake prisoner trick, in which an informer is a cellmate of the suspect from whom the police need information. The informer is a criminal, promised special consideration if he obtains information useful to police.

Career criminals are a scruffy lot, and there's truly no "honor among thieves." At times, some will volunteer damaging information against another to work a "deal" for themselves. One outstanding example was Floyd Wells, a career criminal who brought information to Kansas police that was their first good lead in finding the "In Cold Blood" killers.¹ He told police about statements that his cellmates had made, as these provided leads to solving the case.

Some police agencies, such as the Federal Bureau of Investigation, make extensive use of informers. Agents assigned to criminal cases develop informers, and are constantly seeking more. FBI agents pay money for information, if it checks out, and will even have an informal word with a judge about to pass sentence. There was also a policy of unofficial tolerance for informers' criminal activities, as agents didn't investigate informers "vigorously."²

False Friends

Another type of covert interrogator is the fake friend or sympathizer. This person, who may be an acquaintance, fellow employee, or neighbor, sidles up to you and tries to get you to reveal information useful to the investigation. By pretending sympathy, this type of interrogator can break down the barriers that people normally have, and obtain damaging information.

Undercover Cellmate

This is another variant on the theme. A police officer poses as a suspect, and gets to share a cell with you. Like the genuine criminal cellmate who trades information for deals, the undercover officer will pump you for information. The chances of this happening in the future are greater, now that a court decision (*Illinois vs. Perkins*) has ruled that it's not necessary for an undercover police officer to give a suspect a "Miranda" warning under such circumstances. The decision went on to explain that, although "Miranda" prohibits coercion, it allows deceiving a suspect by use of a fake prisoner. The suspect is not protected against the consequences of boasting about his crimes to people he thinks are fellow felons.³

Undercover Employees

An especially dangerous type is the undercover agent posing as an employee. Certain companies hire private investigators to check on employee honesty, or drug abuse in the workplace. In certain cases, undercover police officers will hire on and conduct investigations, with or without the cooperation of management.

The undercover agent poses as an ordinary employee, and tries to gain the confidence of other employees, while keeping his eyes and ears open. To succeed, he must appear competent in his work, and must have the skill to fit in and do the job. If not, he'll arouse curiosity regarding why he was hired, and why an obviously incompetent person remains in his post.

The agent will socialize with other employees as much as possible, trying to strike a mean between putting himself in a position to obtain information and not appearing "pushy." If

there's a company bowling league or softball team, he'll either join or become an avid hanger-on. He'll pay special attention to cultivating talkative people, or those whose tongues loosen up with alcohol. He'll try to attend parties, to make new acquaintances, and discover weaknesses he may exploit.

You may be naive enough to think that you have nothing to fear because you're innocent. This simply isn't true, because of the secretive, conspiratorial nature of undercover work. If there's a police investigation into drug abuse, and you genuinely don't use drugs, you're not likely to be prosecuted. However, an undercover investigation takes on a life of its own, and can have other results. This is especially true if it's a private venture. A private investigator must produce results to justify his cost, and many are not beyond cutting corners to produce something to relay to their employers.

- The undercover agent may develop other derogatory information about you, which isn't criminal in itself, but which can block promotion or cause other problems for you. An example is your political philosophy. Another is membership in an organization of which management disapproves. Attending meetings of a political, social, or religious organization may get you into trouble. So can books you keep at home, and the inferences a covert investigator may draw from them. You may never know the real reason why you don't get the raise or promotion you'd been expecting, and may never even know you've been investigated.

- The agent may misinterpret something you tell him. In one case, an employee was given a bottle of brandy as a Christmas present by a vendor. Later that day, other employees saw the bottle, and asked him if he'd had a drink from it. He jokingly replied: "I always have brandy in my morning coffee." Minutes later, the company president came to confront him angrily about drinking on the job. The employee was able to show the bottle, still sealed, and explained that a certain vendor had given it to

him that morning. Because there were several others present when he'd joked about the morning coffee, he was unable to pin down who had carried the word to the boss.

- The agent may try to "pump" you for derogatory information about other employees. One sidelight to this technique is to study interpersonal relationships in the workplace, and to question employees about those whom they dislike. It's easy to see that you may easily be willing to spill the "dirt" about a rival, or an abrasive personality.

Covert interrogation is very deceptive, attempting to develop information by stealth. In some situations, though, there's no attempt at subtlety, and the interrogator will proceed at once to torture.

Sources

1. *Notable Crime Investigations*, William Bryan Anderson, Editor, Springfield, IL, Charles C. Thomas, Publisher, 1987, pp. 9-12.
2. *Ibid.*, pp. 205-206.
3. *Law and Order*, August, 1990, p. 12.

8

Torture

Very few people can resist torture. Fatigue saps the will to resist, and physical torture is very fatiguing, because of the pain and the high emotional pitch of fear. Sooner or later, you'll tell the interrogator anything he wants to know. If you genuinely don't have the information he seeks, you'll make up facts to stop the pain. Even if he promises you increased pain if your statements prove to be false, at least fabrications buy you temporary relief. This is why torture is an unreliable method of obtaining confessions. Only in the most backward and despotic regimes are confessions obtained by torture admissible in court.

Another reason why physical torture is uncommon, at least in this country, is that it can produce permanent injury and even death. If you're unlucky enough to be in a situation in which

you may be tortured, you risk being maimed or killed. In some countries, such as Egypt, torture is a routine part of interrogation.¹ This is why you should, if you're facing the prospect of torture, have a very clear idea regarding whether or not the pain is worth it. Are you really willing to risk being severely hurt, and even maimed, to keep the information from your questioner?

Torture in America

However, let's emphasize that physical torture is merely uncommon, but not unknown, in this country. Various laws prohibit obtaining information by physical coercion, but a few police officers break the law. It's hard to say whether physical torture is more likely at the hands of big-city police officers, hardened by unrelenting violence, or by rural sheriffs, accustomed to imposing direct justice.²

Some private security agents also take short-cuts. In fact, it's more likely to happen at the hands of private security agents because these are lower-grade personnel, and usually rejects from a police employee screening program.

As a means of obtaining investigative leads, torture often works. Even if not admissible in court, information obtained under torture can help an investigation, if it checks out. This is why an interrogator will often not go too far with torture, always saving something worse for the subject who lies to him.

Some people may think that they can resist torture, because they've read of heroic secret agents resisting torture by Gestapo interrogators during World War II. According to some stories, these people went to their deaths with their lips sealed. This may have happened once or twice, but a more likely explanation is that a clumsy or cruel interrogator killed them before they could talk.³

Another possibility is that the subject had a severe health problem, of which his interrogators were unaware. Some types of torture are extremely stressful. The ice water bath is severe in effect, causing massive circulatory stress. A person with a heart problem may suddenly die under torture, placing his secrets forever out of reach.

Types of Torture

There are several types of torture. The least common is physical punishment, because lesser measures will often produce information. There are also methods of physical coercion which you may not immediately recognize as torture.

Subtle Physical Coercion

You can expect a short period of preparation before a severe interrogation. Your captor may allow you to drink a lot of liquids, because he knows that this will soon produce a need to urinate, which he can use to his advantage. An interrogator may not allow you to go to the toilet when you need to. If you smoke, one of the first actions of a competent interrogator is to confiscate your cigarettes and withhold them to put pressure on you. If you're a drug addict, or need regular doses of a prescription drug, such as insulin, this is another vulnerable point he'll exploit. Withholding drugs can be fatal, depending on how long the interrogator persists.

There may be a period of waiting, almost certainly in an isolation cell, while the interrogator prepares to begin on your case. The cell may be too warm, or too cold, to induce discomfort and soften you up. An hour or two of sweating or shivering will weaken almost anyone. During the interrogation, you may have to sit on a hard chair, or endure other discomforts.⁴

Severe Physical Coercion

Many interrogators feel that results come more quickly if the subject has time to contemplate what will happen to him. This is one step beyond the initial softening-up in a hot or cold cell.

There will be a few questions to determine if you're willing to talk, and if not, there will be a few mild physical punishments. A few blows can provide a taste of things to come. More important is explaining to you what can happen, to allow your imagination to dwell on and dread the immediate future. A quick dose of psychological coercion goes hand-in-hand with physical torture.

A few simple props are often helpful. Laying some medical instruments out on a table where you can see them is a preliminary to applying torture.⁵

There are many nasty pain-producing techniques, from simple slaps and punches to exquisite technological means such as drugs and electric shocks. Every part of the body is vulnerable. Torturers pull out fingernails, twist their victim's testicles, spray them with tear gas, and pour soda pop into their nostrils.

Some techniques are based mainly on producing fear, rather than severe physical pain. Slapping or punching after an unacceptable answer is one way. Another is to tell the subject that he's about to get a lethal injection, and to actually inject morphine to produce numbness and dryness of the mouth, is another.⁶ Hanging the subject upside-down and telling him that this will eventually blind him can persuade him to talk.

Some drugs cause no physical harm, but produce intense fear. Injecting a paralytic drug based on natural or synthetic curare stops breathing, without causing unconsciousness. A dose of Pavulon or Anectine, administered by a doctor or paramedic, can cause panic in a subject, who remains alert and aware, but

feels himself suffocating. This has been used as a behavior modification technique in some penitentiaries.

Methods of slow torture that cause much pain before actual physical damage are desirable if it's necessary to bring the prisoner to trial, or to release him eventually. Raising the subject by tying his hands behind his back and pulling the rope over a ceiling beam causes discomfort, then pain as more weight comes off his feet.⁷

Another way is to "hog-tie" the subject, with a rope tied around his ankles and running around his neck, tightly enough so that his calves come off the floor. Relaxing his legs will apply pressure to his throat, and he'll begin to strangle.⁸

A way of producing pain without permanent physical injury is with a stun gun. This is an electronic device, costing less than \$100, which produces an alternating current at 20,000 volts or more. This technique is an outgrowth of the "telephone," developed during World War II. The "telephone" was exactly that, a field telephone with a magneto-powered ringer. Spinning the crank would generate a high-voltage current, which the interrogator would apply to the subject's body. Modern electronics provides high-voltage current from a 9-volt transistor battery and a small circuit board.

The stun gun has two contacts, or probes, to carry the current to the skin. A jolt from a stun gun causes intense pain, but leaves no marks, unless the user is careless and allows a gap between the electrodes and the skin. Sparks can burn the skin.

Stun guns have been used to persuade suspects to talk. In one case, in early 1985, a sergeant and a patrolman of the New York City Police Department's 106th Precinct used a stun gun on two drug dealers to elicit information. This was the noted "Torture Precinct" incident, and both officers earned prison sentences for their acts.

These electric torture devices are very different in use from electric-shock machines used in psychiatry. Psychiatric electro-shock involves passing a current through the frontal lobes of the brain, to produce unconsciousness and convulsions. The effects can be moderate to severe, with confusion and loss of memory almost always resulting from each treatment. This is why psychiatric electro-shock is useless for interrogations. Today, its use is limited to treating some cases of depression, and for discipline and control of unwilling subjects. Some backward mental hospitals, as well as some prisons, use intensive shock treatments to make difficult and combative inmates docile and manageable.

Another way of producing intense discomfort is by placing a rag soaked in household ammonia over the face. New York City police sometimes use this technique.⁹

You may be subjected to one or more of these physical techniques, and unless your interrogator is totally inept, they'll be in a definite order. Least harmful techniques come first, with more severe and damaging methods later. The point is to produce information with the least physical damage, and no maiming, if the plan is to release you. If you find your arms and legs being broken, or your eyes gouged out, you can be sure that you're not coming out of the ordeal alive.

Torture is not the best way to obtain information from a suspect, partly because it's legally doubtful, but also because it's unreliable. There are, however, technological means of interrogation, such as the "lie detector." We'll see how this works next.

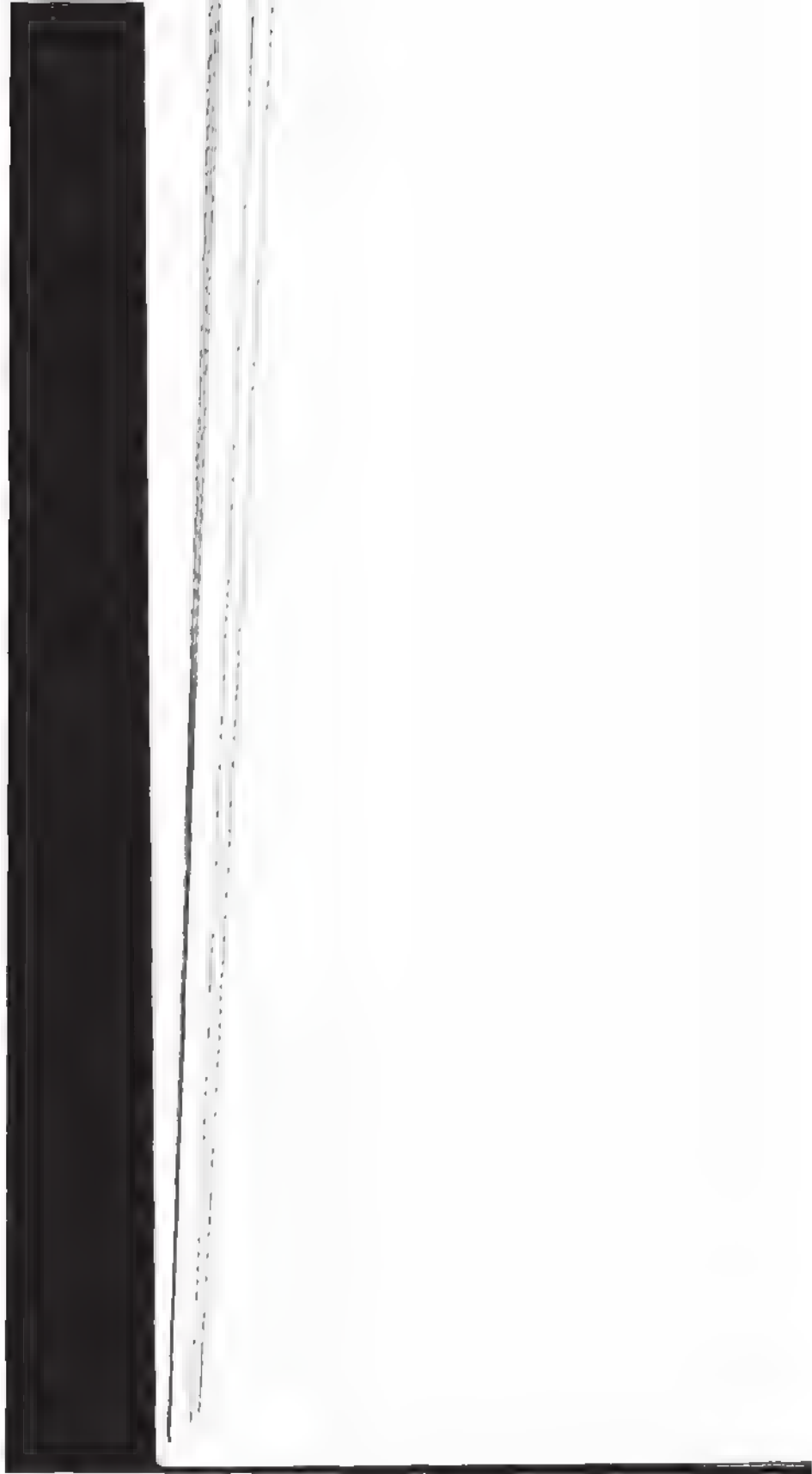
Sources

1. *A Handbook For Spies*, Wolfgang Lotz, NY, Harper & Row, 1980, p. 118.

2. *The Mugging*, Morton Hunt, NY, Signet Books, 1972, p. 106. The case described is that of three Southern Blacks, illiterate and suspected of murder, whom local sheriff's officers had whipped repeatedly until they confessed. This 1936 case, *Brown vs. Mississippi*, resulted in the U.S. Supreme Court reversing the conviction on the grounds that the suspects had been deprived of their rights without due process by the torture.

In another case in the same book, described on p. 113, a New York police investigator clamped a rag soaked in ammonia over the suspect's face, forcing him to inhale the fumes until he lost consciousness. The "third degree" is not totally gone from American policing.

3. *Handbook For Spies*, p. 117.
4. *The Mugging*, p. 107.
5. *Elementary Field Interrogation*, Dirk von Schrader, El Dorado, AR, Delta Press, 1978, p. 24.
6. *Ibid.*, pp. 25-26.
7. *Ibid.*, p. 31.
8. *Ibid.*, pp. 34-35.
9. *The Mugging*, p. 102.



9

The Polygraph

The polygraph evolved during the early years of this century, following the pioneering work of an Italian anthropologist and criminologist, Cesare Lombroso, who had measured blood pressure and pulse rate during interrogation. Several other individuals devised instruments to record heartbeat, blood pressure, breathing and even electrical resistance of the skin, as a guide to determining truthfulness. At the time, the assumption was that disturbances in these would occur if the subject told a lie.

Early History

In 1921, John A. Larson brought out the definitive version of the "polygraph," and his supporters promoted it as a "lie de-

lector." Another notable person in this field was Leonarde Keeler, who improved the device and popularized it through the media. He had a weekly radio show during the 1940s, and made a personal appearance in the film, *Call Northside 777*, to bring his machine before the public. The audience had an opportunity to see a subject with ribbed tubing and wires attached to his chest and arms, all connected to a machine that unrolled a long strip chart that recorded the readings in a series of wavy lines.

The net result is that the polygraph attained wide acceptance in the gadget-happy United States, not because of its merit, but because of public-relations hype. The picture presented to the public was of a scientific and objective instrument that would reliably disclose whether a person was being truthful or not. Several schools sprang up to train polygraph operators, teaching them not only how to operate the device, but also a battery of tricks to use in intimidating subjects. One trick, for example, is to hook up the subject to the machine, and tell him that the charts will disclose if he lies. The operator then lets the subject pick a card from a deck, and the operator asks him if it's the ace of hearts, two of hearts, etc., with the subject answering "no" to each question. After several questions, the operator informs the subject what his card is, implying that the machine spotted the deception. The trick is that the deck used in this stunt is a "force deck," made up of fifty-two identical cards.

How It Works

The polygraph's strip chart records pulse, respiration, blood pressure, and galvanometric skin resistance. If the pulse and blood pressure increase, respiration loses its regularity, and skin resistance drops. These symptoms indicate stress, and the operator interprets this as deception.

All questions in the series require only a "yes" or "no" answer. The operator will usually read the questions to the

subject before the actual test, to start him anticipating and worrying.

The operator asks the subject a series of questions designed to both establish a baseline for the charts, and to measure the subject's reaction to critical questions. "Neutral" questions are routine questions designed to be emotionally neutral, such as "Is your name John Doe?" or "Do you live in New York?" The recordings for such questions establish a level of response for normal questions that don't place the subject under emotional stress.

"Control" questions are designed to evoke deceptive answers. The purpose is to obtain a high-stress baseline, for comparison to questions relevant to the investigation. Examples are:

"Did you ever masturbate?"

"Did you ever steal anything?"

The operator may not, at the outset, know whether the subject masturbated, stole anything, or committed any other specific acts. He can, however, develop a set of control questions by simply asking the subject if he ever committed any of these acts, and then instructing him to answer "no" to the questions during the actual test.

Relevant questions relate directly to the investigation. They may simply take the form of "Did you do it?" but many operators prefer to use a more complicated format. One is called the "SKY" sequence. This acronym stands for "Suspect," "Know," and "You."¹

A typical sequence of questions reads:

"Do you suspect anyone of the crime?"

"Do you know for certain who committed the crime?"

"Did you commit the crime?"

Exact phrasing will vary with the investigation. The questions, in an arson investigation, might all end with "... set the fire?"

Another type of sequence design is the "peak of tension" test. The operator asks the subject questions rotating around the topic, and notes the highest responses. In a theft case, for example, he may ask:

"Is the missing amount between \$1,000 and \$2,000?"

"Is the missing amount between \$2,000 and \$3,000?" etc.

The guilty party will presumably have the strongest reaction after the operator mentions the correct amount.²

Questions are spaced out, with several seconds between them, to allow clear readings of the subject's reactions to each. There will often be neutral questions between relevant and control questions, to get a reading on the subject's overall level of tension.

There may be other questions, to probe the periphery of the investigation. One way to explore other areas is to ask:

"Have you been concealing any information from me?"

Other questions used to probe are:

"Is there anything you stole that I haven't asked you about?"

"Have you been truthful in all your answers?"

"Do you have any knowledge of other acts that we didn't cover here?"

"Have you lied in any of your answers in this test?"

"Have you withheld something important?"

Polygraph operators usually follow up the test with a post-test interrogation.³ In theory, this is to point out areas of strong responses on the charts, and to offer the subject an opportunity to explain them. In reality, this is another way of badgering the subject into a damaging admission. Some polygraph operators routinely bluff every subject this way, whether or not the charts indicate deception at all.

In some cases, the operator will tell the subject that, while he appeared to have answered the relevant questions truthfully, he

showed reactions to some control questions. The pitch then goes like this:

"Just for my own curiosity, can you tell me what you did steal?"

Questions such as these open the door to further interrogation. This is why it's important to be on your guard until you've left the building. The interrogation isn't over until it's over.

How Reliable is the Polygraph?

Most courts don't admit polygraph charts as evidence, because despite various stunts displayed by some polygraph operators, the device's reliability remains unproven. In 1988, Congress passed the Employee Polygraph Protection Act, sharply limiting the use of the polygraph in private employment practice. Up to this point, some companies had subjected all employment applicants to polygraph examinations, as part of the screening process. Using the polygraph had been a cheap substitute for background checks, which can be very costly. Employment managers felt that it was enough to carry out a superficial check of easily verifiable details on the employment questionnaire, and ask the applicant to state under polygraph examination that he had answered all questions truthfully. Some companies also required applicants to sign consent forms, to allow polygraph examination whenever management thought it appropriate. One chain of convenience stores, for example, had a policy requiring polygraph examinations of employees immediately after any robbery. Clerks on duty during the robbery would find that they were automatically the top suspects, and be obliged to report for polygraph examinations.

Police and other investigators continue to use it, because they know it has some value in intimidating naive and credulous subjects who can be fooled by card tricks. In fact, most of the polygraph's successes come before the actual test, when the sub-

ject confesses, rather than allowing himself to be hooked up to the machine.

Police agencies use the polygraph to screen applicants, as a supplement to the background check. This is supposedly an additional safeguard against unsuitable people becoming police officers. However, even the multi-layered applicant screening process doesn't always work.

One police chief of a small Arizona town, exposed as an impostor, had passed a polygraph examination to get his job. He had claimed both military and police experience he did not have, and exaggerated his educational accomplishments. The polygraph operator passed him anyway. The recent case of an Arizona Highway Patrolman, who persuaded a motorist to have sex with him to avoid a traffic ticket, involved an officer who had passed both a polygraph examination and psychological screening before hiring. The Arizona Department of Public Safety placed great faith in these tests, but found that they have their limitations. These cases are only the tip of the iceberg, and there are many other examples waiting to surface. Today, practically all persons applying for police employment must take screening tests or polygraph examinations, and sometimes both. It's worth remembering, whenever a case of a "bad cop" surfaces, that the officer involved is probably another polygraph failure.

One outstanding case of failure was the polygraph testing done on Robert "Bud" McFarlane, President Reagan's National Security Advisor when an article suggesting a leak appeared in the *New York Times*. It seemed that someone in the White House had passed restricted information to the newspaper, and several staffers with access to this information had to take polygraph examinations. McFarlane took the test twice, failing each time, and it appeared that he was the guilty party. He begged the *New York Times* management to tell his boss, the President, that he had not been the one who had leaked the

information. The *Times*' publisher told President Reagan that their information had not come from Mcfarlane, and this cleared his name.⁴

This case is worth studying further, because it holds several lessons regarding how and why the polygraph "works," and shows plainly the problems with the system. First, we can see that anyone who cares about his job and his career will find an accusation of criminal malfeasance very stressful. His pulse and blood pressure will go up when discussing the accusations, whether he's in fact guilty or not. This is also true of people accused of crimes with strong emotional content. Anyone accused of child molesting, for example, is likely to find it very disturbing. A polygraph operator looking for disturbance in the lines on his graph won't have much difficulty in such cases.

The blunt fact is that the polygraph measures the physical results of emotional stress, not truthfulness or deception. The results of polygraph tests are also often not as clear as its proponents claim. If there are many suspects, for example, the polygraph will not zero in on a single person, but the tests will usually result in a short list of "probables." These are people who showed some stress on the charts during the questioning. It also doesn't necessarily follow that the person who showed the most deviant readings is the one most likely to be guilty.

Why, then, do police agencies and various private investigators continue to use the polygraph, and insist that it works? In one sense, the machine does work. Many subjects, when faced with a polygraph examination, will make damaging admissions before the start of the test, because they think that they'll be found out, anyway. They don't know or understand the severe limitations of the polygraph, which is why they get bluffed out. About 75% of employment applicants required to take polygraph examinations made damaging admissions before the start of the test.⁵

In one case, an estranged wife accused her husband of sexually molesting their son. The husband asked for polygraph examinations of both of them, and the day before the scheduled tests, the wife confessed that she had fabricated the accusation.⁶

Fooling The Polygraph

This task has two aspects: fooling the machine itself, and fooling the operator. We'll look at fooling the machine first.

A person intent on deception has several ways to pass a polygraph examination. A person who is particularly nervous or apprehensive can also benefit by studying these methods, because the polygraph, as we've seen, does not discriminate between anxiety and deception.

One quick way to appear less apprehensive, and to blunt the emotional responses, is to take a tranquilizer an hour before appearing for the test. All competent polygraph operators ask their subjects whether they're taking any drugs, prescription or otherwise, because they know that someone under "chemical control" won't respond as intensely to stimuli. This is why, if you're apprehensive about taking a "lie detector" exam, you pop a pill and begin with a lie, denying that you're taking any drugs at all.

One popular tranquilizer that works well for this purpose is Valium. Doses range from two to ten milligrams, but the most effective dose appears to be ten mg. on an empty stomach.⁷ You can ask your doctor for a prescription, stating that you feel nervous, and there's a better than even chance that he'll write you a prescription for what you ask. This is especially true if you ask him for only half a dozen, stating that you feel nervous only occasionally, and that you'd previously found that Valium works well for you. He's less likely to insist on another drug, because

of the small amount and your purported beneficial experience with Valium.

Another drug recommend by an authority on beating the box is Elavil, in doses of 5-75 mg. There were, however, some side effects, including some loss of coordination and concentration.⁸ An alert polygraph operator might notice these.

If you're lucky, you can scrounge a couple of pills from a friend or relative. Either way, you have to find the correct dose for you. This means testing the drug on yourself a couple of days before you take the test, to make sure that it calms you enough, without inducing dizziness or any signs that a polygraph operator might detect. If your only transportation is a car, it's also important that the dose you take isn't heavy enough to impair your ability to drive.

Alcohol will do, if you're in a hurry and have nothing else. If you use alcohol, drink the least aromatic form you can find, which is vodka. If you find the taste of pure vodka too sharp, dilute it with water, orange or tomato juice, or even milk. Chewing gum will mask the slight odor of alcohol on your breath.

Relaxation exercises can also work to reduce stress responses. However, they take time to learn, and practice is essential.⁹

There have been various "biofeedback" devices appearing on the market in recent years. These are solid-state devices to measure pulse, skin resistance, etc., and they can help you monitor your physiological responses to questioning. The main difference between these and polygraphs is that they make no permanent record.

Flattening stress responses is one approach. Heightening responses to neutral and control questions is the other. You can practice several techniques to boost your blood pressure and heart rate upon demand. The thumbtack in the shoe is very well-known, which makes it obsolete.¹⁰ Experienced polygraph

operators will be watching for this, and scrutinizing you carefully to see if you walk with a limp, or favoring one foot, a tip-off that you have to be careful how hard you step.

The best ways are those requiring no gimmick at all. Biting your tongue, tightening your crotch or sphincter muscles, and voluntarily holding your breath are all ways of heightening your responses to neutral and control questions. Do not use muscular tension that the polygraph operator can see, such as gripping the arms of the chair, because he'll be watching for these tricks.

Fooling the Technician

Fooling the machine is only one step. You also have to put yourself across properly to the person who gives you the test. To do this, you have to present the appearance of being both truthful and cooperative.

There are two theories of scoring the polygraph test. One school of thought goes only by the chart, on the assumption that the needle tracings tell all. This allows an expert to interpret the charts of a subject he's never seen, and arrive at an opinion regarding the person's truthfulness.

The other theory is what practitioners call "global scoring." The technician looks not only at the charts, but at the subject's general behavior. Subjects who arrive late, for example, indicate to the operator that they're being uncooperative, and therefore suspect. So do subjects who express skepticism, such as doubting that the machine works. Those who break eye contact, stare at the ceiling, appear nervous, and exhibit other signs of lack of confidence also appear suspicious. Expressing resentment at being required to take the test is also an indicator of deception, the way these people think.

Other techniques which supposedly indicate deception are the "red herring," in which the subject begins arguing the unfairness of the suspicion, accusation, or the test itself. Another type of incriminating statement is arguing over petty details, and claiming that, because there's no proof of every detail, then the subject must be totally innocent. Attacking a witness's motivation or integrity is another tactic, according to this school of thought. Starting extraneous conversations is also another deceptive or obstructive tactic.¹¹

Weaseling statements are also cause for suspicion. These usually take the form of not quite answering a question:

Q: "Did you do it?"

A: "People will tell you that I'm innocent."

This is not a denial of guilt, but an indirect statement that other people will confirm innocence. Deceivers also pepper their answers with other weaseling qualifiers, such as: "...to the best of my knowledge..." or "...as far as I remember..." Others will answer a question with a question, such as: "Who, me?" or "Are you calling me a liar?"¹²

This is why you should be punctual and show the technician a cooperative attitude. Don't express any doubt or resentment regarding the test, his qualifications, or the fairness of the procedure. Act as if you're a totally innocent person, with nothing to hide. However, the best you can do may not be enough. Global scoring is so intuitive, and so imprecise, that an operator who has already made up his mind about you can find a lot of material to justify his beliefs.

One countermove is a clever play for sympathy. A man applying for a security job had apparently made the needles jump when asked if he had a problem with alcohol. In the post-test interview, the technician confronted him with this, and asked him if he had any explanation for it. The reply was that

he'd only the day before heard that his uncle, who had been an alcoholic, had died from cirrhosis of the liver. He passed.

The polygraph is cranky and unreliable. So is the "voice stress analyzer," fashionable a few years ago but now passing out of use. This machine allegedly detected lies by changes in the lower frequencies of the voice, but turned out to be so unreliable that it never attained even the limited acceptance of the polygraph.

Sources

1. *Lie Detection Manual*, Dr. Harold Feldman, Belleville, NJ, Law Enforcement Associates, 1982, pp. 111-114.
2. *Ibid.*, pp. 116-119.
3. *Ibid.*, pp. 174-175.
4. *The Book of Lies*, M. Hirsch Goldberg, NY, William Morrow and Co., 1990, pp. 232-233.
5. *A Tremor in the Blood*, David Thoreson Lykken, NY, McGraw-Hill, 1981, p. 238.
6. Related personally to the author by the intended victim.
7. *How To Get Anything On Anybody*, Lee Lapin, San Francisco, CA, Auburn Wolfe Publishing, 1983, p. 213.
8. *Ibid.*, p. 213.
9. *Interrogation*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987, p. 107.
10. *Ibid.*, p. 107.
11. *Lie Detection Manual*, pp. 174-182.
12. *Ibid.*, pp. 183-185.

Part II:
Special
Applications



10

Prisoners Of War

Prisoners are valuable to their captors because of information they may provide about the enemy's strength, weapons, casualties, morale, and even plans. This is why standard practice is to set up a system of interrogating captives.

Rights of Prisoners of War

According to international law, POWs have certain "rights," but only under certain circumstances. There have been several Geneva Conventions, all directed towards defining the status of POWs, and the treatment they receive by participating nations.

If you're a military person captured by enemy forces, the treatment you may expect will vary depending on several con-

ditions. The Geneva Convention is not universal, and not all nations in the world have signed it. Historically, nations which have provided the most humane treatment to POWs, partly because they are signatories and partly because of tradition, have been the Western nations. We're not likely to be at war with Britain or France in the foreseeable future, and may instead be fighting in the Middle East or Asia. Nations which have not signed the Geneva Convention have their own rules, and generally they treat POWs harshly.

Another condition is whether or not there's a declared war. American fliers shot down over North Vietnam were surprised and dismayed to find their captors telling them that, as the United States was not at war with North Vietnam, they did not qualify for POW status. Instead, they carried the label of "criminal." If you're captured during an undeclared "police action" or other type of intervention which is not a fully declared war, your uniform may not protect you.

The Geneva Convention applies only to war between nations, not to internal security functions, police actions, or civil wars. If you're involved in one of these, don't be optimistic about your prospects if captured.

It also applies only to members of the armed forces in the sense that they are the only ones allowed to fight under its terms. Civilians are non-combatants, and as such, they're not allowed to take up arms against the enemy's armed forces. A set of rules governs treatment of civilians, who are not allowed to be used for military labor, as hostages, etc. Any civilians who fight, in a guerrilla or underground movement, forfeit their rights under the Geneva Convention. If you're a civilian fighting against an occupation army, expect them to treat you as a criminal if they capture you.

This is true of any nation, even the ones we consider very civilized. In Northern Ireland, members of the Irish Republican Army do not get POW status when captured. On the contrary,

they get put on trial for their "crimes," as if they were street criminals. In the United States, members of various "liberation armies" have faced trial and imprisonment upon capture.

Certain practical conditions also affect what you may expect if captured. If you're a flier who has just been bombing the enemy's homeland when shot down, you may face some very angry people who may not be at all interested in your information, only your blood.

Military Interrogation Goals

There are many purposes to military interrogation. The most important and universal one is to squeeze you for information. You may face questions about your unit, officers, weapons, tactics, and other details of your organization. This is "front-line" or "tactical" intelligence, which is information immediately useful to the battlefield commander.

There are also longer-range objectives, such as forming strategic estimates of morale of your armed forces, or morale and will to fight in your country. This is information that isn't as urgent, and is the concern of interrogators at POW camps.

Another purpose is to use POWs for propaganda. A few POWs who sign a declaration that the war is unjust can generate favorable propaganda for their captors. POWs who sign confessions of atrocities can also help their captors.

Military Interrogation Tactics

There are several types of military interrogations, for different purposes and locales.

"Field Interrogation" is to obtain immediately useful information. You may, if captured, expect this within a few

minutes or hours of being taken prisoner. An intelligence officer will question you in a dugout or tent, not far behind the lines, to get what he can as quickly as possible. He may simply question you, or may threaten force if you remain unresponsive. You may face a severe beating, with broken teeth and bones, or a quick execution, if you don't cooperate.

"Shock Interrogation" overlaps with Field Interrogation. Here, the theme is speed, to put questions to you while you're still shocked by your capture, and before you can regain your mental balance and begin adjusting to captivity. An important part of shock interrogation is to keep you isolated, especially from countrymen who have also been captured, to deny you mutual support. Once you're in a camp with other captives, the value of shock interrogation is far less.

"Interrogation by Deception" takes many forms. An enemy may pose as an officer in your armed forces, to question you regarding your activities before capture. You may find enemy officers handing you a "Red Cross Form," to allow them to notify your family that you're alive and well, although a prisoner. The form contains many questions not relating to your family, but instead covering military information.

Some interrogators use "killing with kindness." This involves simply being nice, thoroughly solicitous of the POW's needs, and being consistently polite. The interrogator may wear a uniform of the corresponding service, but a grade higher than the POW. The session does not begin with an interrogation, but as an invitation to tea or dinner. Small talk over the meal produces relaxation, and may lower the POW's guard. As a fellow sailor, or airman, the interrogator can discuss service matters professionally with the POW, and by gradually leading the conversation around to military topics, may be able to obtain the information he seeks. This technique served both British and German interrogators well during the last global war.

Once you're in a formal prison camp, you'll be under several different types of pressure from your captors, aimed at getting your cooperation in several different ways. Some tactics will also deal with alienating you from your buddies, to keep you emotionally isolated.

Another set of tactics involves necessities and amenities of life. If you're wounded, your captors may tell you that medical care is rationed, and available only to those friendly to the regime. They may offer you medical care in return for your expression of friendliness, in the form of information or a confession.

Physical discomfort can break down both morale and health quickly. One harsh tactic is to keep the POWs in small cells or boxes, without food or water, for several days at a time. Forced to sit in their own excrement, they soon weaken and become ripe for interrogation based on a system of rewards.¹

Food, clothing, and heating fuel are also media of exchange. You may find the prison camp diet inadequate, and learn that you can earn an adequate ration by cooperating with your captors. In cold climates, you'll find your barrack room cold, and you won't have enough blankets, unless you give your captors what they want. Mail to and from home is also a medium of exchange, and you might find that only letters which contain statements favorable to the regime ever reach your family. Your captors might also withhold mail from home, until you agree to cooperate.

"Salami Slicing" is a variation on the theme. Your captor doesn't try to get you to provide information or to sign a confession immediately, instead offering rewards to those who attend an "orientation" lecture. This is in a comfortable room, and he serves refreshments after the lecture. He may follow this with a "study" period next day, with rewards to those who can pass a test on the topic studied. The rewards continue, and each step in cooperation is so small that it's hard to draw the line and begin refusing.

All of these are proven techniques based on principles of behavior modification. They don't work equally well with everybody, but they work.

Tactics For Prisoner Management

Prison camp administrators need to keep their captives docile and compliant, to help the interrogators with their job. They do this by using several means to lower their captives' morale.

"Managing the News" is common. The camp administration controls all news arriving in camp, especially news from home, to keep the prisoners feeling isolated and forgotten. If an armistice is imminent, the prisoners don't hear about it, unless it serves a purpose for the interrogators.

Suborning prisoners is also common. In any group, some are stronger than others. Camp administrators seek out the weakest ones, and apply intense pressure to obtain their cooperation. This gets a foot in the door, and other POWs who see a few benefiting from cooperation may also be tempted.

Breaking the chain of command is another tactic to reduce prisoner morale and cohesiveness. When camp administrators see group leaders emerging among the prisoners, they transfer or kill them. Officers are not allowed contact with the men, and regular executions prevent the development of any sort of prisoner organization.

Cultivating informers is especially valuable, because few things break down morale as quickly and thoroughly as knowing that someone wearing the same uniform is betraying you. The most important part of such a program is letting the prisoners know that their words and actions are the subjects of reports to the administration from within their own ranks. Letting a few tid-bits of information slip is one way to increase anxiety.

Another is developing a fake informer. This works if prisoners regularly face interrogation and beating. The administration selects several who are particularly hostile and uncooperative, and calls them in for "interrogation," one at a time. Instead of suffering questioning and beating, they simply sit in a room alone for a couple of hours. At the end, each gets a chocolate bar or pack of cigarettes, and is allowed to leave. Other prisoners will quickly notice that some come out of interrogation sessions without any marks or bruises, and with small gifts. This creates suspicion quickly.

Surviving POW Interrogation

American servicemen have to obey a code of conduct, which prohibits giving an enemy useful information, or cooperating in any action harmful to the United States. This originated after the Korean War, during which American servicemen in Communist hands embarrassed their government by signing confessions and denouncing American war aims. 7,190 Americans spent time as POWs during the Korean War. 2,730 died in captivity, and of the survivors, 13% collaborated with their captors, some giving in after only a few minutes.²

The code of conduct requires American servicemen to continue fighting while they still have the means to resist, try to escape if captured, and to avoid saying or doing anything that would benefit the enemy. They must not provide any information beyond their name, rank, and serial number, and must not give their "parole" that they won't try to escape. POWs also must maintain a chain of command, and obey their superior's lawful orders.

The problem with this code of conduct is that the people who wrote it, and who require American servicemen to follow it, are not the ones behind the barbed wire. It's easy to sit behind a desk

and write regulations that cold and starving men thousands of miles away are supposed to obey. In practice, human resistance can go only so far. The experiences of POWs in Vietnam showed the limits.

In a short war, with POWs in captivity for only a few weeks or months, morale doesn't suffer as much, and it's easier to resist when your health is still good and you expect release soon. Your captors, as well, probably will be mindful of the prospects of retaliation if they mistreat you. If the war lasts for years, with poor food, no news from home, and no prospects for release, your morale will suffer greatly.

It's even more difficult if you're injured. Physical injury is weakening, and recovery is longer and more difficult on a marginal diet.

There are still some survival measures you can take. One is to discard rank badges, and try to pass for an enlisted man if you're an officer. Enlisted men, in principle, have less information than officers, and this may spare you some intensive interrogation.

Important to survival is your awareness of the tricks enemy captors may use against you. Trust in your fellow prisoners is very important, and you must be aware of the ways the enemy will try to divide you by creating distrust. At the same time, it's important not to discuss classified military matters with fellow prisoners. They don't need to know the details of any secret equipment you operated before capture, and anyone who tries to get this information from you may be a plant or an informer.

It's also wise not to draw any conclusion about informers without proof. Some may appear to be collaborating, or passing information, but an accusation of treason can be devastating to camp morale.

Don't try to hold your own courts-martial and executions of those whom you suspect of treason. It's illegal under the Geneva

Convention, and the enemy can put you on trial as a common criminal. Save your testimony for later, after you're back home, and tell what you know to your superior officers. It then becomes their problem, and they'll have the resources to handle it.

Finally, you must understand that there are some situations which you won't be able to handle. An example is being taken as a civilian engaged in sabotage or resistance. Military Intelligence, or the civilian secret police, will be able to do what they want with you, including execution without trial.

Sources

1. *Interrogation*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987, p. 190.
2. *Techniques of Persuasion*, J.A.C. Brown, Baltimore, MD, Penguin Books, 1963, pp. 283-284.



11

Pre-Employment Interviews

These interviews are among the more stressful experiences Americans undergo, except for the hereditary rich, who don't need to work. Despite the vast number of pre-employment interviews personnel managers conduct each year, some remarkable fakers slip through the process.

One of the most notable fakers was Ferdinand Demara, Jr., who faked his way into several high-level jobs in the United States and Canada. He became a Canadian Navy doctor, professor at Pennsylvania's Gannon College, law student, zoology graduate, teacher, and a monk. His career was so outlandish and remarkable that Hollywood made a movie about him, starring Tony Curtis.¹

Let's look at the pre-employment screening process, which involves several stages. Getting a job is truly running the gauntlet, with a series of obstacles to overcome.

Posture

Remember a few basics about job-seeking. These will direct your answers to certain questions, and help you to be consistent. We'll call this your "posture." Use it as a guide when tailoring your answers for specific employers:

You are competent. You can do the job. Other employers have paid you because you did the job well for them.

You have suitable qualifications for the job you're seeking, which means not too many and not too few. If the job requires a college degree, you must state that you have one. By contrast, don't appear "over-qualified," as this will block employment. In fact, an employer might wonder why someone with a master's degree is seeking a job frying hamburgers. The practical point is that the employer will feel that you'll work for him only until you can find something better.

You generally get along well with other people. You do not have personality clashes or conflicts with fellow employees or with supervisors.

You express a positive attitude towards former employers and supervisors, demonstrating this by praising them. This shows that you got along well with them.

Your career has been upward and onward. Each job you left was for more money and benefits. Each job should reflect more income. The exception is if you were laid off, or your employer went bankrupt. In such cases, it's reasonable to accept the same or less pay, just to get a job.

You are normally cheerful, and don't have any serious problems, mental or physical. You also do not worry much.

You are outgoing, and prefer activities that bring you into contact with other people. You prefer bowling, for example, over stamp collecting.

Whatever you do, don't allow yourself to feel intimidated or discouraged. Remember that you're competing for the job, but not usually against the cream of the crop. No matter how much puff a prospective employer puts out about his company's high standards, and how he hires only the best, the fact remains that if he paid enough, he'd already have the best working for him. You're only competing against a limited field.

Resumes

This isn't a chapter on how to write resumes, because you can obtain that information from other books. Instead, it's going to deal with the uses of a resume, and make you aware of certain pitfalls.

You can use a resume for two purposes:

1. As a door-opener to mail to prospective employers. This is routine, and often a waste of time unless you're responding to a specific classified ad or other indication that there's an opening.
2. As a crib sheet when filling out employment applications. Wait a minute! If you present a resume, why would an employer want you to fill out an additional form?

The reason is that most resumes don't tell an employer what he wants to know about you. A "functional resume" lists your skills, but doesn't go into detail about your employment history. In the same manner, a "chronological resume" lists your employers, but is unlikely to list how much you earned at each job,

or your reasons for leaving each. Employers want this information, and you can be sure that they'll ask you.

Another reason is that many resumes are carefully edited versions of the truth, designed to make you look as good as possible, while concealing weaknesses and vulnerabilities. Many people puff up their careers in their resumes, which is why many employers and their personnel managers feel that 50% of a resume is bullshit.

One form of "faking good" is the "Apollo Syndrome." The name comes from the person who served the coffee to scientists and engineers at Cape Kennedy during the Apollo launch, and who claims credit for its success because his coffee kept them awake to do their jobs.²

Employment interviewers also look for puffed up language, such as "implemented" and "directed." These may mean that the applicant was in charge of an important program, or that he simply shuffled papers. To avoid suspicion, use simple language that directly describes your responsibilities in each job.

Also avoid listing diplomas from obscure colleges, unless they're real and you have a copy with you. There are many diploma mills in this country, and employers are wise to this trick.

One way of scoring points is to state that former employers sent you to training courses and seminars. This shows that they thought well enough of you to invest money in special training.³

You can do this by choosing several areas in which you're very skilled and claiming that you gained your expertise at special courses. Employers never check this out, as reference checking usually consists only of verifying college degrees and former employment. You must, however, have the skill to back up your statements. The worst mistake you can make, in this regard, is to state that you learned everything you know on the

job. Lack of any academic background counts against you these days.

Yet another point is to be specific regarding dates of employment and separation. Simply listing the year isn't enough. One authority points out that, by listing only the year, what appears to be continuing employment may conceal a gap of up to a year. If you're going to list a job, list both year and month, and preferably the date, as well. This avoids leaving an obvious gap, and avoids giving the appearance of concealing information.⁴

Applications

The next step in the employment screening process is the application form. In one sense, it's actually not very important, because all it does is present a framework for the interviewer to use in formulating questions. However, mistakes in filling out the application can be fatal to employment prospects! The reason is that many people admit too much, assuming that the prospective employer will find out all damaging information, anyway. This is a false assumption, as we'll see.

Fundamentally, you can provide any information you wish on an employment application. Follow your resume exactly when filling out the employment application. Remember that your resume and the application are the basic tools the interviewer will have, and that practically everything else he'll use or develop will come from information you provide him. Let's run over a few rules regarding employment applications, and how to build a good background for yourself:

1. **Be prepared!** This is the vital first step. You must have your story straight in your own mind, and be ready to deliver it in a convincing manner. With employment applications, the first step is to fill one out at your leisure, so that you

can massage the weak spots without being under a time limit. One way to do this is to pick up an application from a potential employer and ask if you can fill it out at home, as you have another appointment right then. Another way is to obtain employment application blanks from an office supply store. Yet another way is to apply for a job you don't want, and as soon as they hand you an application form, walk out with it. Make several photocopies as work sheets, and try several sets of answers to create the most credible background for yourself.

2. Do not provide any derogatory information in the employment application or any paperwork you fill out for any employer. NEVER! NEVER! NEVER! Do not admit to having been fired, using alcohol or drugs, or having any criminal convictions. If they want the dirt, let them dig for it! They usually don't, as we'll soon see.
3. When filling out any application or questionnaire, be realistic, and use common sense. This means not to try to "fake good" so much that you present an image of an angel or a "Dudley Do-right." It's all right to admit that you take an occasional drink. It's also permissible to know an alcoholic or two. You may even admit that you had an uncle who drank to excess. However, absolutely deny that you hang around with anyone who uses illegal drugs. You may admit having known such people in high school or college, because a denial would be incredible unless you attended a religious school. However, be careful to state that none of your current friends are dopers.
4. In some cases, you may need to cover a gap, such as a job from which you were fired, or time spent in prison or a psychiatric hospital. As a rule, the further in the past this gap is, the easier it will be to cover. One way is to list a totally fictitious job, with a company that no longer exists. If you have been working in the same field for some years,

you probably know of a real company that folded. The only problem you may have is encountering a former employee. The interviewer may tell you; "Come and meet Joe Blow. He used to work for the same company, and now works for us. You'll have a few things to talk over, I guess." In such a case, excuse yourself politely, and leave. You won't have much hope of faking your way through that unless you know something about the company and those who worked there. If you do, you may be able to bluff Joe Blow.

Another way to cover a gap is to claim employment out of state, or out of the country. Be careful, however, to have enough background to do this. If you claim you worked in Paris for two years, yet can't speak a word of French, you may meet someone who does. If you don't know the layout of the Paris subway, or the city's basic geography, and encounter an interviewer who does, you may be stuck for an answer if he asks you questions about Paris.

You may also claim to have worked for a relative. This is usually 100% secure, as an investigator often won't bother to ask a relative for any information. The best bet is a relative with a name different from yours, to mask the kinship. Your relative may even be willing to confirm your fictitious story.

Yet another way to cover a gap is to claim to have been hospitalized, or seriously disabled, for that period. If you have a limp, or other noticeable handicap, it's simple to list the time disabled to cover the questionable period. Remember to be precise with dates, to avoid suspicious questioning.

5. Faking higher education is also fairly easy, if you know what you're doing and the job requires a degree. You won't be able to fake a specialized education, if you're applying for a job as a biologist or machinist, without the

skill. However, claiming a bachelor's degree in liberal arts is a snap, if you're well-spoken. You may even be able to claim a master's degree, in some cases. Always make sure that your educational credits are from fairly well-known institutions.

Background Checks

Although employers like to state or imply that every item of information on an application is subject to investigation, this is often only a ploy. Don't worry much about being unmasked by a background check. Many employers or employment interviewers are lazy or over-worked. It's surprising how many of them totally omit checking information which they could verify with a phone call.

Thorough background checks are also time-consuming and costly. Most employers omit them, or only spot-check their applicants. Some depend upon national investigating firms that specialize in providing background checks on employment applicants through their information networks. However, these companies deal in volume, and their background checks are superficial. This is why it's stupid to admit any damaging information at the outset.

Many applicants are worried sick that derogatory information will eventually come to light, and they confess all on their applications. Realistically, there's less chance of derogatory information coming out today than ever before, because of several lawsuits by former employees against employers who provided derogatory information to personnel investigators. Companies have had to pay damages because they impaired former employees' ability to obtain employment. This has chilled the atmosphere, and today hardly any employers will provide any information beyond verifying dates of employment, and possibly salary range.

The situation is so extreme that at least two nurses, suspected of killing ward patients, were able to find other employment because the hospitals for which they'd worked were afraid to badmouth them when prospective employers asked for references. Genene Jones, for example, had been suspected of killing patients in the pediatric intensive care ward of Bexar County Hospital, in San Antonio, Texas. She nevertheless was able to obtain employment with a Kerrville, Texas, pediatrician, because staffers at Bexar County Hospital kept quiet about their suspicions.

Another factor can work in your favor if you're thinking of leaving a job where you're having bad relations with your employer. In practically all cases, your employer would prefer that you leave voluntarily, rather than forcing him to fire you, because if you quit, his unemployment insurance premiums don't increase. It's also less troublesome to have an employee leave on good terms, rather than angry, because of the increasing numbers of reprisals taken by hostile former employees. Some commit sabotage before leaving. Others return to vandalize the property. One angry ex-employee returned to the printing company that had fired him in Louisville, Kentucky, and shot up the plant and personnel.

Some things are not subject to verification, because they lead to dead ends. Claiming employment with a defunct company leads an investigator to a dead end in most cases. Don't, however, list a totally fictitious company. Some investigative agencies keep back copies of telephone and city directories to check this out, because this trick has been used before.

Another important reason for giving only casual attention to the background check is the employer's or interviewer's ego. It should not be surprising that these people consider themselves experts on human nature, experts on "reading" and handling people, and experts at outwitting employees and employment applicants. After all, they're the successful power people, aren't

they? If you're looking for a job, that makes you dependent on them, and places you in an inferior position, correct? Many employers make the mistake of thinking that, because someone who works for them is a subordinate, he's an inferior as well.

Let's look at a concrete example of how this works. Martin John Yate, author of one of the best books on interviewing and hiring practices today, lists eight reasons why some employers hire unsuitable people, including poor screening, poor interviewing, and poor questioning methods. Last on the list is failing to check references.⁵

Yate devotes most of his book to coaching the reader on how to spot inconsistencies and problem areas in a resume, and how to probe the applicant's personality with adroit questioning. The underlying theme is that the interviewer is smart enough to spot falsifications, and the applicant is not smart enough to outwit a conscientious interviewer. In the real world, this happens every day.

The Interview

There are several types of interviewers you may face in your job hunt. One is the interviewer working for a state or private employment agency. These agencies are known colloquially as "body shops," because their main purpose is to move bodies. Their interviewers do the basic screening and send people who might be suitable to the employer. Such interviewers are often very low-quality people, especially those working for private agencies. Because they work on commission, they earn more money if they move more people. In their effort to refer people, they routinely misrepresent both the candidates and the employers.

You might feel gratified to hear such an interviewer describe you in glowing terms as he sets up an appointment for you with

a prospective employer, but don't think for a minute that you've fooled him. He's just building up your image so that he can collect his commission.

You may be surprised to find that he's misrepresented the job to you in certain ways, such as citing a higher salary than it actually pays. If you ask him for an explanation, the standard reply is that the figure included benefits as well.

The other type of interviewer works for the company's personnel department. This person does the final screening, to ensure that only suitable candidates take up the supervisor's time.

The final person is the employer or supervisor himself. This is the person who makes the final decision regarding whom he'll hire. In small businesses the employer must be his own personnel department, and you don't face any intermediate interview.

Most professional employment interviewers aren't very bright. If they were, they wouldn't be holding down such poorly-paying jobs. They do, however, hold power over some of their fellow human beings, and they make the most of this. There are some who enjoy the power, and relish stomping on a person who is in a poor position to defend himself.

Most of this power is illusory. Personnel managers and interviewers are not the ones who make the final hiring decisions. As we've seen, they only do the preliminary screening. Still, in their role as gatekeepers, they have the power of first refusal, and they can make it hard on anyone who doesn't please them.

In this way, they're much like the arrogant telephone receptionist who insists on knowing what your call is about before she'll put you through. Occupying one of the low positions on the totem pole is frustrating, but some manage to take out their frustrations on people more helpless than they.

This is why many personnel people play mind games with their interviewees. They pretend to have special insights, attain-

able by using special psychological tricks, to select suitable people for their employers. Unfortunately, this intellectual masturbation doesn't serve any purpose but to confuse the entire process.

You may find the interviewer asking you a series of questions that appear meaningless, or unrelated to the job. Questions about your hobbies, for example, don't appear to be job-related at all, but some interviewers think that your hobbies reveal how social a person you are, and how well you get along with others.

Think about this if the sort of job you're seeking is one which requires public contact, or working with other employees. If an interviewer asks you what your hobbies are, don't say that you follow anything intellectual or that you can do alone, such as reading, or building model ships. Instead, mention bowling, playing cards, or any other activity that requires teamwork, or at least interaction with people. But if the job is a solitary one, such as monitoring gauges in a power plant, interpersonal relations aren't as important.

Keep in mind that many interviewers feel that a person's attitudes are guides to his or her behavior. If asked how you feel about people who steal from their employers, or who use illegal drugs, you must state that you strongly disapprove, and that you feel they ought to be punished. Any tolerance you show will lead the interviewer to suspect that you're either defending them because you're a druggie or a thief, or that you're on the verge of doing it.

Some interviewers are outright incompetent or lazy. This is the sort of interviewer that will ask you closed-ended questions, such as "Were you happy in your last job?" Only a fool would answer that he wasn't, because that would open the door to questions about how well he gets along with employers.

Here are some closed-ended questions that you should always answer with "yes," regardless of any skeptical manner the interviewer might adopt:

"Do you get along well with people?"

"Do you get along well with your supervisors?"

Here's a short list of closed-ended questions that require only a "no" answer, no matter how close to the truth they come:

"Were you ever arrested?"

"Were you ever fired?"

"Have you ever refused to obey your employer's orders?"

"Did you ever steal on the job?"

"Did you ever pass your company's proprietary information to unauthorized persons?"

"Do you use drugs?"

"Have you ever been to a psychiatrist?"

Another type of unskilled interviewer uses the ultimate open-ended question: "Tell me about yourself." The worst possible answer to this one is the question: "What would you like to know?" because it shows lack of poise. The proper answer is to describe your work experience, without quoting from your resume or application. Simply explain how you started in your field, and what you learned at each job. Tie it in with any special training for which your former employers paid.

You may encounter a skilled interviewer who uses "layered" questions. In asking about a specific area, he'll ask about different aspects of the same topic. For example, you might find him asking you these questions, in sequence:

"What was your main responsibility in your last job?"

"How did you handle it?"

"How many departments did you have to deal with in handling that?"

"What was the easiest part of handling that?"

"What was the most difficult aspect of handling that?"

"Did you have to work much overtime at it?"

Another layered sequence might relate to likes and dislikes:

"What did you like best about your last job?"

"What did you like the least?"

"Why?"

"How did you handle it?"

"Give me a specific example."

Layered questions are very probing, because a quick and superficial answer won't do. They're designed to expose the faker, and they work fairly well.

Another type of question you may hear is the negative or "stress" question. This is designed to force you to tell about your weaknesses. Some examples are:

"When was the last time you faced a problem you couldn't solve?"

"What duties do you like the least?"

"What do you find most difficult to do?"

"What is your weakest point?"

"What kind of decisions are hardest for you?"

"Why aren't you earning more?"

"What was it you disliked most about your boss?"

These test your poise, because you must answer them. You can't simply deny them all. You might state that you got along well with all of your supervisors, but you would not be able to make a credible case that you had always liked everything about every job you'd ever had.

The way to handle such questions is to put a positive spin on your answers. Reply that you don't like jobs in which you're not allowed to work to your full potential, that your weakest point is your impatience to get the job done, etc. The hardest decision for you should be which employees to lay off when the order comes down for a cut-back.

Discriminatory Questions

It's illegal to ask questions relating to race, national origin, religious affiliation, political beliefs, etc. However, some employers still do, either directly or obliquely. This may not be offensive if you're the "right" religion, and this helps you get the job. If you're not, and you feel that the employer is discriminatory, you have to make a decision. Unfortunately, it's a decision that requires you to consider several aspects.

First, do you really want that job? Do you want to work for a person who would hold your religion or ethnic background against you?

Secondly, is the job so tempting that you'd want to sue or bring a complaint to the Equal Opportunity Employment Commission to get it? Would you be able to work in a place where you'd gotten the job through legal action?

Thirdly, is the effort worth the trouble, considering the time it will absorb? Can you afford to wait many months for a job, knowing that you might lose your case in the end?

When you consider all of these factors, you'll be able to decide whether you want to make an issue of discrimination, or to seek employment elsewhere.

Rehearsing

The best way to learn which specific questions you're likely to face is to apply for jobs you don't really want. This will give

you experience in interviewing, and practice in answering questions. You'll find it an enjoyable experience, because you won't have the nagging anxiety that often comes when your job depends on the results of the interview.

The other purpose that these dress rehearsals serve is to desensitize you. You'll get to feel more comfortable with practice, and when you go to interview for real, you'll feel more confident and at ease.

These dry runs also provide you with experience regarding employers in your area. You'll find out how closely they check references, for example. One way is to apply for several jobs entirely out of your field, and provide a totally faked employment history, to see how far you can go. You might get tripped up when an employer asks you specific job-related questions, but don't be surprised if one or more actually offers you a job.

Pre-employment interviews can appear intimidating, but in most cases they're not the free-for-alls that interviews with the media can be. Let's now examine the problems and pitfalls of talking to the press.

Sources

1. *The Book of Lies*, M. Hirsch Goldberg, NY, William Morrow and Co., 1990, pp. 205-206.
2. *Hiring the Best*, Martin John Yate, Boston, MA, Bob Adams, Inc., 1988, p. 44.
3. *Ibid.*, p. 87.
4. *Ibid.*, p. 46.
5. *Ibid.*, p. 19.

12

Media Interviews

Some people who have dealt with the media have horror stories to tell about being misquoted and unfairly treated. The reason is that some media people practice "advocacy journalism," slanting the news to support an evangelistic viewpoint. Others simply seek the most sensational aspect of a story to promote, in an effort to build their audience.

"Advocacy journalism" means that the reporter manages the news to push his or his editor's viewpoint. Selective reporting is a powerful tool, and is one way of slanting the news. In various forms, it's the foundation of advocacy journalism. You can't fight advocacy journalists, but you can avoid making their jobs easier.

Libel laws won't protect you if the media decide to do a number on you. There are ways of misrepresenting you that are above the law, and media people know all the tricks. The result is that you have to take steps to protect yourself. The first step is to understand why and how media people work, and the various stratagems they use to obtain damaging interviews.

Giving Your Side of the Story

If you're involved in a controversy, or any type of litigation, a reporter may approach you with the stated purpose of giving you an opportunity to get "your side" across to the public. This is the same trick police use, and it's a cheap ploy to get you to talk. The reporter may even tease you with hints regarding what's allegedly been said about you. If you're suggestible, you may easily fall for this one.

Biased Language

Some interviewers try to disparage you or your viewpoint by describing it in uncomplimentary terms. If you allow them to do this during an interview, you'll lose right at the outset.

Let's hypothesize that you're being interviewed after shooting someone who tried to hold you up on the subway. The reporter asks you: "How many vigilantes like yourself do you think are riding the subway?" If you let this slip by you, and allow the reporter to get away with labeling you a "vigilante," you'll put yourself in a bad light. The way to handle it is to tell the reporter forcefully: "I am not a vigilante. That's your term, not mine."

Off The Record

At times, a reporter may ask you a question, set off by the phrase, "off the record." This purportedly means that he won't

publish what you tell him, or attribute it to you. You accept such an assurance at your own risk. If you're a political candidate, and you believe a reporter's assurance that he'll treat your candid opinion of your opponent as "off the record," you may be surprised by a headline that states: "Smith Retarded, Says Jones."

Your statement might not make the headlines, but the reporter might use it as a lever to pry a statement from your opponent. This is especially true if you're being interviewed on camera. The reporter might also violate his promise to you, and run it in his news program.

Let's put this in capital letters, to burn it into your memory:

**NO INTERVIEW IS EVER OFF
THE RECORD IF IT'S ON TAPE.**

A TV interviewer might have the nerve to tell you that what you say to him is off the record, but as long as the camera's running, it's going on tape, and you might see it again on the six o'clock news. His promise to you, of course, will not be on tape.

The other side of this is that an unscrupulous reporter can use your off the record words to pry a statement out of your political opponent. Even without being involved in politics, your words can return to haunt you. An example is the reporter working on environmental or workplace hazards. If you blow the whistle on your employer, even off the record, you run the risk of having your words kick back in your face. If you divulge information known only to a few, and the reporter confronts your employer with it, it won't take much effort to figure out the source of the leak.

The best investigative reporters work very hard at protecting their sources, because they know it helps build their credibility. The only way to be sure of avoiding problems with statements

made off the record is to speak only with well-known media people with track records of not "burning" their sources.

The Ambush Interview

This is a favorite tactic among some pushy TV reporters. You emerge from your home or office to face a TV camera, and a reporter puts a microphone in front of your face and starts asking questions, without even introducing himself. If you get flustered, and say the first thing that comes into your mind, you'll probably say something you'll regret.

There's only one way to handle the ambush interview. Turn around and walk away. Don't acknowledge the reporter or the cameras. Don't say "No comment," because that produces a bad impression on TV. Don't even face the camera, once you see it, because that suggests you're cooperating in the interview. Simply turning your back, remaining silent, and totally ignoring all questions destroys the ambush interview, and sends the reporter down in flames.

Remain Silent

The simplest way to avoid giving a reporter ammunition he can use against you is by keeping your mouth shut. "Silence Cannot Be Misquoted" is a good principle, and is the title of a book by the former press secretary of a politician who was savaged by the media during his career. It can be very hard to keep your mouth shut at times, because media people are very adept at persuading people to speak with them. Without police or subpoena powers, they cannot force you to talk, and they have to use guile instead of coercion.

In approaching you for an interview, a media representative may be very friendly and sympathetic. If you consent to the

interview, you'll first hear a series of questions designed to get you off your guard. Near the end, you'll hear hostile questions.

A hostile question is one framed to put your actions, and your responses, in the worst possible light. This is the "Have you stopped beating your wife?" type of question that makes you appear guilty before you can answer. No matter how you answer it, you won't look good.

The only way to combat this type of treatment is to know with whom you are dealing. Never accept an invitation to an interview from an unknown. You and your press secretary can often tell, by scrutinizing the work of various media people, which ones are fair and which are merely seeking sensationalism. In fact, certain television interviewers have built reputations for hammering their interviewees, and these are the ones to avoid. A number of newspaper columnists are also noted distorters of fact, and their bias is obvious from reading their columns.

If in doubt, keep your mouth shut! This is especially important if you can't think on your feet. Remember, you're up against pros who know every verbal trick to elicit the information they want, and who know how to frame questions to control the answers. Unless you can match their skill, you're facing an unequal contest.

The Final Cut

This is a TV term, and it signifies the final edited version of a program, the one which goes on the air. It's the electronic equivalent of editing, or selecting the material to present. The final cut is a powerful tool, because it allows a TV reporter, or his editor, to delete portions of an interview in which you look good, and include only those which show you hesitating, or saying "No comment."

One way to cope with this is to insist on control over the final cut yourself. This is a condition which few TV persons will accept, but it's an effective way to keep them from hammering you.

Media interviews can be harrowing, but you can fake them out. More difficult, however, is when you have to answer questions under oath. Sworn testimony is more intimidating, but it's also possible to handle it, as we'll see next.

13

Depositions And Court Testimony

These are special situations, because every word you say goes on the official record. You're also under oath to tell the truth. Before we get into the nitty-gritty of sworn testimony, let's lay out a few points about attorneys:

1. Your attorney works for you, and you should be able to tell him everything relevant. You should be candid with him, because only if he knows the weak points of your case will he be able to forestall moves by the opposing attorney.
2. Your attorney's job is to represent you, and to get the best deal for you, whether the case is civil or criminal, and whether you're innocent or guilty. Guilty people are entitled to legal representation, too, under American law.

3. In a criminal case, you may be surprised to find your attorney not asking you if you're guilty. In some instances, he really doesn't want to know. His job is just to do the best he can for you, guilty or innocent.
4. In a criminal case, if your attorney is "Legal Aid Society" or otherwise court-appointed, don't expect too much. They're overworked, and they know that most of their clients are guilty, anyway. The most you may expect, as a rule, is that your attorney will try to cut the best "deal" he can with the prosecutor. You may be surprised to discover that at least 90% of criminal cases in this country include a "deal" in their dispositions.

There are all sorts of attorneys, in both civil and criminal fields. In civil practice, you will always want an attorney with you if you have to attend a deposition hearing. This is essential, because the attorney questioning you may try to bluff you into answering questions without legal justification.

Depositions

These are question-and-answer sessions, under oath, during which you are obliged to answer the attorney's questions. You may have your attorney present, and he may object to improper questions, but a deft interrogator won't let this stop him.

The trick is "staying alive" during the question-and-answer session, and to present the appearance of truthfulness. At the moment, the only person you have to "sell" is the other side's attorney. If he thinks he's on to something, or that he can get you to reveal something you're trying to conceal, he'll come at you very forcefully. On the other hand, if he feels that you've been truthful, and that there's nothing to be gained from attacking, it will show in both his manner and the content of his questions.

The basic principle is the same as during interrogation: never give anything away.

Let's quickly review the basics of giving testimony, either in court or at a deposition hearing:

1. Look at your questioner, or at the jury.
2. Listen carefully to the questions, and think before answering.
3. Speak up, so that he, the judge and jury, and the court reporter can hear you.
4. Answer positively, without hedging.
5. If you don't know the answer, say so simply and directly.
6. Never change your testimony, or contradict anything you have said previously. This can be very important if you've previously made a written statement, and the attorney questioning you is going over the same ground. Never decide that you have a better answer now than before. Never assume that the attorney knows something to contradict your previous statement. Even a questioning look, raised eyebrow, or sidelong glance is totally insignificant, because it doesn't show in the court transcript.¹

If you hesitate in responding, you can be sure that the attorney will notice this, and begin working around the question, asking you the same thing in a dozen different ways. If you don't answer the question, or if you hedge, he'll also take this as evasion. You can tell when he's zeroing in on the vital issue.

On the other hand, if the other attorney wastes time asking you routine questions about your address, where you lived before, your education, etc., he's simply marking time. He may try to ask you embarrassing questions, such as whether or not you've been to prison, confined in a psychiatric hospital, etc., but unless the answers are relevant to the issue, he's just trying to impress his client. Attorneys often use such posturing to

convince their clients that they're earning their fees. You still have to be careful, though, because if you get caught in a lie on routine questions, you can be in for a hard time.

Note that the most important phrase is "get caught." Never assume that the other attorney knows more than he actually does. Don't assume that your previous statement wasn't good enough, and that you need to change it. Your statement may appear weak to you, or even have some obvious flaws, but only a contradiction is the kiss of death.

You can often get by with a weak case simply by repeating what you'd said previously. The other attorney may not pick up on the weak points. If you have a confident manner, you can "sell" yourself to a judge, jury, and even to your opponent's attorney.

This is why you've got to "sell" the other side's attorney the idea that you've got nothing to hide, or at least, that it's forever beyond his reach. A good analogy is a safe to which you're the only one who knows the combination, and he can't prove that you know it.

Courtroom Testimony

The main differences between giving testimony at a deposition and in court are that court is more formal and structured, is larger, has more people present, and there's both direct examination and cross-examination. The attorney for the side for which you're testifying (remember, you may be a witness to a crime, civil action, etc.) will ask you questions about what you saw, heard, read, etc., to bring out the points he wishes. The opposing attorney has a chance to ask you questions of his own, to probe weak spots in your account and to open gaps in your testimony.

The direct examination is friendly questioning. Cross-examination is hostile, to break down or cast doubts upon your testimony. The attorney for your side should go over your testimony with you before your court appearance, and anticipate possible attacks from the other attorney. You ought to discuss these frankly with your attorney, and if there's anything you know that might adversely affect the case, bring it out before entering court. Don't leave any points as surprises to pop up during your testimony or cross-examination.

Perjury

Perjury means lying under oath before an official body, or in special situations, such as deposition hearings. Perjury is a crime, and many prosecutors and attorneys use the threat of prosecution to coerce their subjects into providing the answers they want to hear. In reality, there are very few prosecutions for perjury, because it's truly a hard crime to prove, and few prosecutors try.²

Perjury is also often not worth prosecutorial effort, especially in domestic cases, such as divorce or custodial hearings. Everyone knows that in emotionally involved cases feelings run high, neither party is objective, and both parties shade the truth somewhat. It's simpler to overlook much of it, and allow a certain quota of lies.

For these reasons, perjury is often your best shot. The main points, when considering perjury, are how important the case is, and how can the other side prove that you knowingly lied. The other side may know that you're not telling the truth, but proving it is often hard to do.

If you're testifying in a case involving organized crime, there may be 50 investigators ready to run down evidence of perjury. If it's a divorce action, it's typically one party's word against the other's. Neither side has the people or the financial resources to devote to a massive effort.

If the perjury is a denial, the critical problem is what other evidence exists on the topic. If you're denying, for example, having written a certain check, there may be a check with your signature floating around out there, waiting for someone to scoop it up and introduce it as evidence. There may be one or more witnesses who saw you write it, who received it, or who saw someone else receive it. If any of these witnesses are close enough to find and bring to court, they may shoot down your testimony.

If faced with contradictory evidence, you can no longer stand by your story. In conceding, you have several ways out, although the other attorney, the judge, or the jury may not believe you. One is faulty memory. You might state that the incident took place so long ago, or was so insignificant, that you had forgotten it. This may work, in some cases, and save your credibility regarding other testimony.³ However, you'll have lost that particular point, and opened the door to the other attorney's asking you if you're having another loss of memory regarding another point at issue.

The second way is to maintain that the question was unclear, or that you did not understand it. It can take some fast footwork, but you may be able to get away with it:

"Oh, you mean while I was living at home, before I moved out!"

"I thought you meant during my last job, not this one."

Contradictory evidence is not always there. This brings us back to self-contradiction. This is the only way in which you can do a number on yourself, and hand the adversary a victory on a platter. Keep your story "straight" and it won't happen.

Sources

1. The author learned this lesson the hard way, but fortunately without paying a heavy price, during a deposition hearing relating to a divorce. The attorney was going over the answers to a questionnaire previously completed by the author, and at one point the author contradicted his written statement, thinking that the attorney might have had other information. Fortunately, this serious error was about a minor point that didn't surface again during litigation.
2. *The Book of Lies*, M. Hirsch Goldberg, NY, William Morrow and Co., 1990, pp. 34-35.
3. This can also kick back at you hard. One woman was faced with contradictory evidence regarding her date of birth, which she had falsely stated in a previous sworn statement. This led to several uncomfortable minutes during which she had several whispered conversations with her lawyer, but finally had to explain the discrepancy.

Part III:
Resistance



14

Coping With Interrogation

We've covered various types of interrogations and interviews, and the range of tactics you're likely to encounter. It's now time to tie it all together, enabling you to design your plan to resist interrogation.

As we've seen, refusal to talk or answer questions is practical in only a few instances. When applying for employment, you cannot stand on your Fifth Amendment rights, for example. You therefore have to decide upon a basic stance, and a course of action, to guide you during the session. In a criminal investigation, you may decide that it's better to appear cooperative than to stonewall the investigation. Central to this is your personality

How Well Can You Resist?

As a start, examine your personality and behavior to form an appraisal of how well you might resist interrogation. Remember that interrogators like to see someone who is easy to manipulate, suggestible, and willing to talk. They probe for weaknesses to exploit. Nobody's perfect, and it's better to be aware of your weaknesses beforehand than to find them out during an interrogation, as a questioner takes you apart.

To find out your potential vulnerabilities, take this self-test to check out your weak spots. Think carefully about your answers, and be honest, because nobody will know but yourself. Answer the following questions about your behavior:

- Can you stand silence, when with another person, or do you feel a need to break the silence and say something?

If you can't stand silence, you're very vulnerable to an interrogator's staring at you, and making you uncomfortable enough that you start speaking.

- Are you very talkative?

If you are, it will work against you, unless you're an absolute chatterbox. Spilling every detail to an interrogator simply makes his job easier. However, if you constantly change subjects, interrupt yourself in mid-sentence, and return to ask him what he originally wanted, you can make it very hard for him to follow you, and you'll tire his mind quickly.

- Do you listen carefully when another speaks to you, or do you just wait for him to finish so that you can say something?

If you're eager to speak, you might find yourself blurting out something you later wish you hadn't said.

- Do you crave attention, or do you prefer people to ignore you?

If you crave attention, you'll be more receptive to an interrogator, especially if he "softens you up" first by leaving you alone in a room for hours.

- Do you contact your friends and acquaintances, as a rule, or do they call you?

This indicates whether you need people more than they need you, or vice versa. If you need human contact enough so that you're the one who initiates the contacts with friends and acquaintances, you're more vulnerable than you would be if people came to you. This is a dependency vulnerability.

- Are you suggestible? If someone tells you: "Look at that," do you immediately turn your head?

If you're very suggestible, this can work against you during interrogation, because the interrogator can exploit it to control your behavior. If he spots this weakness, he may take advantage of it by approaching you in a slow walk, flexing his muscles and scowling. Intellectually, you know that he's not going to attack you, but on a more basic and emotional level, this provokes fear.

Suggestibility also makes you more vulnerable to various deceptions employed by interrogators. Fake line-ups and identifications are more likely to prey on your mind.

- Do you snap out your answers to questions?

If you reply without thinking, you'll be especially vulnerable for two reasons. First, you won't be considering either the question or your answer carefully, and this leads to errors. The other reason is that sooner or later there will come a question that is truly probing, and you'll hesitate in answering. The interrogator will pick up on this, and know that he's hit upon a sensitive area.

- Do you often feel the need to explain and justify yourself?

If you do, you're very vulnerable to the interrogator who intimidates you with an accusing manner.

- Are you the "nervous" type, and do you show it by gestures and movements of the hands or feet?

As we saw several chapters ago, many interrogators believe that someone who blinks, looks at the ceiling, crosses his arms, etc., is deceptive. If you are normally fidgety, you'd better be aware of it, and understand the impression it makes on an interrogator. As we'll discuss later, you may want to practice appearing calm, or do relaxation exercises, in preparation for an interview or interrogation.

- How good is your resistance to pain?

You're not likely to be "worked over" in most situations, even in many foreign countries, but there are exceptions. In certain extreme situations, an interrogator may resort to force, and this can be very persuasive.

- Do you have a criminal record?

This is vital in determining how investigators treat you. A record is a very large black mark against you, if they know of it.

- What is your ethnic background?

To some, it will appear racist, but investigators go by common experience, which tells them that a Black man is more likely to be involved in street crime than a Caucasian. By the same token, if the crime is embezzlement, or stock fraud, they'll probably be looking for Caucasian suspects.

- What's your socio-economic level?

If you live in the ghetto, you're more likely to face abuse from investigators, because of the assumptions that you're uneducated and don't know your rights, and that you cannot afford a private attorney. Both police and private investigators know that legal-

aid lawyers are too overworked to represent most of their clients properly, which gives investigators more latitude in their tactics.

Avoiding Emotional Isolation

We've seen how police interrogators, by getting subjects away from familiar surroundings, or by taking advantage of a stressful situation, can break down a subject's resistance. Emotional isolation, being away from friends and relatives, can be devastating, and you should avoid it at all costs.

In practical terms, this means avoiding interrogations in unfamiliar surroundings, such as a police station. Many police investigators, even if they have no grounds for an arrest, prefer to invite a subject to their offices, where they can control the environment. They also like to separate the subject from his friends or relatives, or anyone else who might provide emotional support. Another reason, which they don't like to admit, is that they are lazy.

The basic rule for you to follow is that any questions they have for you may be asked on neutral ground, such as the sidewalk in front of your home. You should also try to have someone with you while answering police officers' questions. An attorney is best, but lacking an attorney, a close friend who is hard to intimidate is suitable.

A police officer will do his best to separate you from your friends or relatives. He may insinuate that anyone present is somehow an accomplice, or that he can start investigating them as well. This tactic may intimidate some people, but if you and your friends know your rights, you can cope with it.

If arrested, try to get a lawyer and bail as quickly as possible. Refuse to speak with police officers without a lawyer present. In this limited respect, you're in the driver's seat. The police have

to be correct in their relationship with you. Failing to advise you of your rights, or failing to obtain the proper warrant if one is needed for a search, can throw their entire case out of court. By contrast, you don't have to be right. If you don't want to talk, they can't hold it against you in court.

Police and other investigators have little tricks to put their subjects at a disadvantage. One is to ask you: "What do your friends call you?" and then address you that way, in a false show of intimacy. The best reply to such a question is to ask: "Why do you want to know?"

Cooperation

In some situations, it's better to appear to cooperate with police. This is when you're actually isolated, such as being stopped by an officer while you're alone. In such a case, it's best to answer his questions, and avoid antagonizing him in any way. The reason is that you're extremely vulnerable alone with a police officer, because whatever happens, it's your word against his. He may claim that you assaulted him, and that he had to subdue you. Unless you're 60 years old and infirm, you'll have trouble finding a judge to believe otherwise. Without witnesses, a court will probably accept his version of the events. If you end up under arrest anyway, wait until you see your attorney, and tell him what happened. In such a case, the claim that you confessed to avoid being beaten is worth presenting in court.

Also very relevant is your personal history. If you're a white-collar employee or a professional with a "clean" record, police will have a harder time making a jury believe that you were combative than if you're a vagrant with a record of violence.

Presenting A Credible Front

It's not enough to plan to resist interrogation, because in many cases it's unavoidable. We're repeatedly facing questions about

our backgrounds, employment records, daily work, and other mundane topics. This is why it's important to work hard on building a credible persona, a front that inspires confidence. Let's go over some factors that people use to judge the truthfulness of others. In so doing, let's keep in mind that the overall impression we present is as important, if not more so, than the response to a particular question. Professional confidence tricksters know this, which is why they work hard at presenting an appearance of respectability.¹

Eye Contact

Many sources, both authorities in the field and ordinary people, feel that maintaining eye contact is crucial. Failure to keep eye contact, or "shifty eyes," is a popularly accepted symptom of deception.² The most successful liars and con men know this, and cultivate a straightforward look, and will even stare into the other person's eyes.

Another aspect of eye contact is how people react to various types of questions. Try this on a wife or friend. Ask your helper to say his name or address. Watch the eyes, and note which way they move. Now ask him to multiply 11 times 12, and do a few other sums. Do his eyes move differently? Does the person stare up into the air, while calculating? Most peoples' eyes move differently when giving a response that requires thought or calculation instead of simply reciting from memory. This is supposedly a way of distinguishing invented answers from truthful ones.

The reasoning behind this theory falls down easily, when we think that many untruthful answers don't require much thought. The reply to the question, "Did you steal.....?" is simply "No."

A more complex reply, such as one explaining one's whereabouts during the time a crime took place, may require invention, but a clever liar will have his answer prepared and rehearsed.

Yet another theory is that the pupils dilate under stress, and this can betray a lie.³ The problem with this theory is the same as the others: stress does not necessarily denote a lie. However, if someone thinks you're lying because he sees your pupils dilate, it's still trouble for you.

Speech

There have been controlled experiments regarding how speech patterns change when someone is lying. Allegedly, a person lying slows down, and the pitch of his voice rises. There's also an increase in slips of the tongue, and an increase in bridging sounds, such as "um" and "uh."⁴ This, again, shows an increase in anxiety and stress, but not necessarily untruthfulness. Controlled experiments are not parallel to actual conditions, such as a person's trying to avert suspicion of a crime.

Liars also allegedly force smiles when they lie. This is sometimes obvious, especially when there's an evident pattern of deception, but it also is a symptom of embarrassment. Sweating is also a sign of emotional stress, which some interrogators interpret as proof of deception. Both can mean simple nervousness. Common experience shows this very clearly.

Disarming Candor

A poor tactic is to try to "fake good" about everything. Nobody's perfect, and many interviewers test their subjects' truthfulness by questioning them about personal faults, such as whether they were ever late to work, or ever took home any company property. While it's wise to deny having been fired, or having a criminal record, it's pointless and stupid to deny minor faults. Most successful interviewees understand this intuitively,

and adopt a pose of disarming frankness. This means cheerfully admitting to having made small mistakes, giving an impression of candor. Let's look at one way to handle a question, using disarming candor:

"Have you ever been late for work?"

"Yes, once I forgot to set the alarm, and I was two hours late. My boss was very nice about it, and didn't chew me out. I felt so badly about it that I made sure I was never late again."

This makes several points. First, it shows "honesty" in admitting a misdeed. Secondly, it portrays good relations with a former supervisor. Thirdly, it shows that the subject learned from his mistake.

Don't go overboard in admitting faults. It's allowable to admit small errors and various character traits, but a major error to admit to anything serious. This is especially true if you're being interrogated on a criminal matter.

Never admit to a criminal record of any sort. Many investigators are lazy, as are civilian interviewers, and prefer to have their suspects do their work for them. Admitting to having been arrested or convicted simply leads to more incriminating disclosures. Your chances of concealing a record are not as bad as many think. First, the National Crime Information System is glutted with records, and contains a percentage of errors and omissions that is a closely guarded secret. Your record might simply have gotten lost. Your chances are even better if your conviction was in another state. The record will be only in the NCIC, and not in your present state's computerized memory. If your record is very old, it might never have been entered into any computer.

Some investigators are thorough, and some are simply lucky. A check might turn up a conviction, and the investigator may use this against you, accusing you of lying to him. Your comeback is simply that you were innocent. You didn't mention it

because, despite the conviction, you didn't actually do it. If the investigator insists that you were guilty, reply that your conviction was overturned on appeal. He's not likely to check this out, unless you're under suspicion of a very serious crime.

Finally, don't contradict yourself. This is so crucial that you must take extra steps to ensure that it doesn't happen. Run over your statement in your mind before appearing for any interrogation or interview. This is easy to do when seeking employment, because you have ample time to compose and review your resume, and fill out employment applications. In a criminal setting, you may not have the time, and you'll have to think on your feet and keep it simple. This is true whether you're guilty or innocent.

Police investigators, attorneys, and other interrogators know that showing a subject a contradiction in his statements is often a pry-bar to "breaking" his story. This is why they question suspects for hours, going over the same ground again and again, until the tired suspect makes a mistake and contradicts himself.

There are several ways to cope with this tactic:

1. Tell the interrogator that you're tired, and want to stop.
2. State that you won't make any statements without your attorney being present. Your attorney will coach you, and help you cope with the questions.
3. Purposely misstate several answers, to show the interrogator that he's not going to get any more useful information from you. Make sure that your misstatements are not about critical facts, though.

Assertiveness

You also need to be assertive, without being offensive. This is walking a fine line between sticking up for yourself, so that an interviewer can't bulldoze you, and being too aggressive, so

that he feels that you "come on too strong." You have to show poise.

Always remember that some people are power-oriented, and see relationships only in terms of power politics and intimidation. In an interview, they'll test you to see if they can push you around.

The main rule is to be polite, both in manner and choice of words. You'll find this balance necessary to counter some verbal tricks interviewers use. Let's get into the nitty-gritty of using assertiveness to avoid being bulldozed.

Some interviewers like trick questions, loaded questions, and other subtle and unsubtle manipulative techniques. Some like word games because of the feeling of power they get from using them, while others feel that dishonest questioning has tactical value.

An example of a dishonest question is the "predicated question," or "leading question," asking something based on an assumption, in the expectation of forcing an admission. Psychologists love to use this trick, when they ask: "At what age did you first masturbate?" An employment interviewer may use a variation on this theme by asking:

"When were you last fired?"

"Tell me about the last argument you had with a supervisor."

This is where you have to calmly and politely contradict the interviewer, and explain that you've never been fired, or that you never argue with a supervisor.

A situation demanding quick assertiveness is the silence following a feedback statement. The interviewer will repeat a word, phrase, or sentence from your last statement, and sit and stare at you, as if expecting an answer. If you've just told him that you managed a prototype program in your last job, he may repeat "Prototype?" and look at you.

If this happens, there are two ways of handling it.

The first is to nod and say, "Yes, prototype."

If he refuses to move on to another question, and continues to stare, give him a few more seconds, to be polite. Then ask him: "Do you have any other questions?" as if the interview may close right then. Another way is to ask: "Can I ask you some questions?" If he agrees, you then pose questions about the company, its benefits, etc. This is the polite way of regaining control of the interview. If he wants more information, he'll have to ask you for it.

Some interviewers try to hit you with reflexive questions, making a statement followed by "Don't you agree?" The way to handle this, if you don't agree, is to tell him that you're not sure of his meaning, and ask him to explain further.

A reflexive question may be designed to suggest the answer, but for a devious purpose. The interviewer may be probing for the applicant's views, and testing his sincerity at the same time. It's a sort of test, loaded against the applicant, because to give the right answer, he has to buck the interviewer. Coping with this may appear tricky, but the technique is actually very straight-forward. Let's look at an example:

Q: "We think that telephone follow-up should begin within ten days of after we place an order, don't you?"

This is one of those maybe questions, because the answer could go either way. The safe course is not to contradict the interviewer, but show him that there's another way, and express your willingness to do things his way, if he wishes. Here's how you might answer him:

"Where I worked before, my supervisor had me always send out a follow-up letter, and I only phoned if the vendor didn't answer the letter promptly. What procedure would you like me to follow here?"

This answer doesn't contradict him directly. Instead, it shows that you followed another procedure because it was standard at your previous job.

Some interviewers are addicted to "stress interviewing," which is a technique of keeping the subject off-balance with tough questions. This has some justification if the object is to test the subject for ability to stand up under pressure relevant to the job. An applicant for a media or public relations job may have to be able to think on his feet, and retain his poise in difficult situations.⁵

This can backfire, however, by antagonizing the candidate. One qualified individual took such offense at the way he was treated that he stated emphatically that he would never work for that person.⁶

Body Language

Hand movement also supposedly betrays the liar. The person whose hands move a lot, especially if rubbing the face, is supposedly a liar. Unfortunately, this, too, is uncertain. There are cultural variations in hand movements.⁷

The major problem is that many interrogators accept certain types of behavior as symptoms of deception. Some authorities even list these symptoms for their disciples to read.⁸ If you encounter one of these, and you happen to be the nervous type, you'll appear deceptive to him.

You can, however, correct some of these behavior patterns. A basic step is to learn to practice relaxation exercises. You can use these before interrogation, and even during the session. If it's a criminal interrogation, you can be quite open about it. When the interrogator sees you squirming, tell him forthrightly that you're doing relaxation exercises because you've never been a criminal suspect before.⁹

Preparation

In most cases, you'll have ample time to prepare for the session. If you're job-hunting, have a friend ask you likely questions before you go for an interview. While it's not possible to anticipate every question an interviewer might throw at you, you can get an idea of which questions are in vogue in your area.¹⁰ Simply go for a few dry runs, applying for jobs you don't really want, to gain exposure to current interviewing practice.

Rehearse your answers. Go over the questions you think an interviewer will pose, and try different answers to each, so that your friend can form an opinion regarding how well they come across to him. Rehearsing your answers will also produce "desensitization" to any anxiety that the topics may produce. Your blood pressure may, for example, jump at the question: "Have you ever been fired?" or "Have you ever stolen anything?" After practicing saying "No" or "Never" a few dozen times, you'll find yourself calming down.

When rehearsing your answers, don't try to polish them word-for-word. Interviewers may pick up on answers that seem too pat, and this can alert them to something wrong.

Another point to watch, both when formulating your answers and when responding to surprise questions, is to give a direct answer, if you can. Never evade or equivocate. If an interviewer asks you if you've ever been convicted of a felony, never answer the question with a question, such as "A real felony?" or ask him to repeat the question. Never say, "No, not really," as this sounds weak. Simply say, "No." If he asks a question to which you don't know the reply, simply say, "I don't know."

This point is critically important. Direct answers always present a more confident front than any sort of qualified answer. Saying: "I suppose so," or "I'm not that sort of person," sounds weaseling, and even a bored or stupid interrogator will quickly

pick up on this. If you can answer a question with a "yes" or "no," do so.

The best policy is to provide short answers, just long enough to answer the question adequately. It's not necessary to explain, if a simple "yes" or "no" will do. In fact, volunteering information can often sound defensive, and defensiveness implies that there is something which needs defending.

Tactical Resistance

Just as there are tactical systems in interrogation, there are systems for resisting. Unless you refuse outright to talk, you'll have to hold a dialogue with your accusers.

Resistance can be total or partial. Total resistance is simply refusing to discuss the case at all. It's all right to ask for food, water, and other amenities.

The first, and simplest, step is outright denial. Deny, deny, deny, and claim that they've got the wrong suspect. This isn't too bad a tactic to use, because interrogators expect it. If you cave in and tell all right away, they may think that you're trying to con them, and they'll continue probing to uncover the "truth."

One way to counter an interrogator's appeals is to shake your head "no" whenever he begins to speak. This non-verbal language makes it clear that you're totally rejecting everything he's trying to tell you. Even the most verbally skilled interrogators can't defeat this tactic by words alone. An unskilled interrogator will lose his poise if you use this tactic against him.

Another way is to appear confused. Contradict yourself on innocuous points, to create doubt in the interrogator's mind regarding your reliability as an informant.

Exploiting Interrogators' Mistakes

The fundamental point here is to be familiar with interrogation tricks and tactics, and to be ready to use them against the interrogator when you can. If you're familiar with the various tactics, both straightforward and deceptive, that interrogators use, you have a road map of the interview. When you notice the interrogator begin one of the standard tricks, you can prepare a counter-move. Sometimes, it pays to refuse to respond to a trick. In other cases, it may be helpful to pretend to be fooled.

The "good guy-bad guy" trick, with one interrogator harsh and demanding and the other pleasant, is very old, but it still works with some people. You may choose to counter it by treating both the good guy and the bad guy alike. You may also seek to exploit this trick in your favor. The technique is to appeal to the good guy when the bad guy leaves the room. You might say something like this:

"Look, I really didn't do it, but how am I going to convince him of that? He's just out to get me."

Another point is to try to glean information from what the interrogator asks. Listen carefully to every word of every question. The reason is that questions themselves often give you clues regarding what your interrogators already know. If, for example, you're asked, "On what day did you go to the empty warehouse to hide the money?" the question reveals that they know about both the empty warehouse and the money.

Poorly-trained, unskilled, or over-confident interrogators often say more than they should, giving away information to their subjects. This is how they contaminate an interrogation. It's bad to blab, whether you're on one side of the fence or the other. Try to build a picture of what they know, and what they don't know, so that you can limit yourself to admitting only what they already know.

Advance Preparation

Prepare as many answers in advance as you can. This will give you a more confident manner than if you have to invent answers on the spur of the moment. If you're trying to describe a person or place, don't try to invent someone or some place with which you're totally unfamiliar. If you state that you saw someone running away when you found a dead body, describe someone you know well instead of inventing a description. Remember that you may have to repeat your description several times, and that you must be fairly consistent.¹¹ The exception to this, of course, is if an event took place in light too poor to allow a good view of the person.

If you're presenting an alibi, be sure of your details. For example, if you say that you were at a movie at a certain time, be prepared to state the title of the film and to provide a synopsis of its plot. It's safe to expect that they'll check. Likewise if you claim to have been in another city at a critical time. Don't mention a city you've never seen, because you can expect to be asked where you stayed, where you took meals, and other questions to test your familiarity with the locale.

The back-up story is always a possibility if your story breaks down. This is a common and well-known trick used by spies and professional criminals, but it still works, as does the "good guy-bad guy" ploy interrogators use. To avoid confessing to what you really need to hide, you tell a story against yourself. If you have to explain your presence in a certain restaurant, you can say that you were meeting a married woman. The sleazier the circumstances, and the worse light they cast on you, the easier it will be to get the story believed. This is especially true if your interrogator has a dirty mind and a taste for raunch. A good whips-and-chains story may convince him, and distract him

from pursuing the real issue. If you really want to get raunchy, you can say that you were involved in a homosexual pick-up. It beats confessing to murder.

Don'ts

Don't volunteer information. If you can answer a question with a "yes" or "no," do it, and don't add anything unless asked. Always remember that supplying additional information leads only to more questions. If the interrogator wants to know something, let him ask about it directly. Make him work for his money.

Don't display a sullen silence, unless you've refused to talk until your attorney arrives. An interrogator will interpret silence as a way of concealing something, and will hold it against you.

Don't adopt a super-calm manner, devoid of emotion. An "iceberg" manner turns people off, and provokes resentment. It's also not normal, because people react and show emotion in certain situations. If your questioner is a psychologist or psychiatrist, he'll interpret an iceberg manner as "flattening of affect," which is a symptom of schizophrenia. Remember, an appropriate emotional response always works in your favor, not against you.

Don't allow the interrogator to feel, by your manner or by your statements, that you think yourself smarter than he is, or that you look down upon him. You'll antagonize him, and he'll only cause you problems later. A superior attitude can win the battle, but lose the war.

Don't be flip during questioning. This can easily give the impression that you don't take the business seriously, and antagonize your questioner. The personal equation is very

important, and if your interviewer feels that you don't show proper respect, he'll resent it.

Don't play smart-ass, to an interrogator or to anyone else in an official capacity. You may be tempted to do this, if your attorney gets you bail and frees you from police custody, but resist the temptation. If you antagonize a police officer or a private investigator, you'll make it a personal matter, and he'll remember you. Much later, he may get an opportunity for "payback."

Don't shoot your mouth off, either to an interrogator or to someone whom you consider a "friend." Remember that one of the investigator's most useful tools is the informer, and that the person to whom you are revealing damaging information may be itching to run to the interrogator to repeat what you tell him. Always remember the "need to know" principle.

This last point is crucial, because there's an emotional let-down after an interrogation is over. We've already seen how some interviewers use this period to induce a subject to drop his guard. If you relax while still in the interrogator's presence, or with someone whom you falsely think is on your side, you may reveal something inadvertently.

Sources

1. *The Rip-off Book*, Victor Santoro, Port Townsend, WA, Loompanics Unlimited, 1984, p. 21.
2. *The Book of Lies*, M. Hirsch Goldberg, NY, William Morrow and Co., 1990, pp. 233-234.
3. *Ibid.*, p. 234. Also *Law and Order*, August, 1990, p. 95.
4. *Ibid.*, pp. 234-235.

5. *Hiring the Best*, Martin John Yate, Boston, MA, Bob Adams, Inc., 1988, p. 74.
6. *Ibid.*, p. 74.
7. *Telling Lies*, Paul Ekman, NY, W. W. Norton Co., 1985, pp. 105-109.
8. *Criminal Interrogation*, Arthur S. Aubry and Rudolph R. Caputo, Springfield, IL, Charles C. Thomas, Publisher, 1980, pp. 244-255.
9. *Interrogation*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1984, p. 214.
10. Personnel interviewing is a trendy art. Simply asking job-related questions is old-fashioned, and modern interviewers try to be clever, following whichever theory is fashionable at the moment.
11. *A Handbook For Spies*, Wolfgang Lotz, NY, Harper & Row, 1980, p. 122.

15

The Language Of Lies

A relatively new field in the behavioral sciences is linguistics, the study of the use of language, and the hidden meanings in choice of words. This has application in general and clinical psychology, and in criminal investigation.

Studying the language of a statement can disclose a person's educational level, familiarity with the language, possible foreign origin, and in certain cases, signs of mental disorder. Scrutinizing the structure and content of a statement can also provide clues to deception.

The theory is that the way a person expresses himself gives indications of truthfulness or deception. This is so obvious that it needs no scientific proof. A person who answers a question with a question is evidently evading the question. So is one who

deflects the question by giving an inappropriate answer. Others hedge their answers, or claim not to remember the facts in question. These behaviors are cross-cultural, and do not depend upon a particular language or even level of education. An educated person will, obviously, be able to compose his answers in more sophisticated language, but the same purpose and principles apply.

Tactics of Deception

Most people are fairly truthful, in the sense that they won't tell an outright lie. Instead, they'll provide answers in weaseling language, glossing over relevant facts, and withholding relevant information. The reason is that they want to avoid committing themselves to an untruth.

Both structure and content are important. For example, the use of pronouns often discloses something about the relationship when describing the actions of two or more persons. A clerk describing a stick-up, for example, is more likely to say: "The gunman took me into the back room," or "He took me into the back room," than "We went to the back room." Using separate pronouns reinforces that the clerk and the gunman are not allies, but adversaries. "We" would be inappropriate in this case, because it would imply that they acted in conjunction.

A change in the use of pronouns in a statement indicates a change in the relationship. It sometimes happens that a victim begins actively cooperating with a captor. It can also indicate a period of emotional stress. A victim's statement might begin with:

"He came in and pulled a gun from his pocket. He said it was a stick-up, and I raised my hands. He moved over to the cash register."

In discussing his feelings during the episode, the victim may well shift pronouns:

"When something like this happens, you feel it's not really happening to you. You see things in a daze, and nothing seems real."

There may be gaps in the narrative, which the subject fills by phrases such as "afterwards" to bridge time, and "We talked," without indicating what the conversation contained. These are indications for further questioning.

A statement's contents can also provide clues to deception. A general rule is that the person who experienced something experienced the entire event, not only the details important to the investigation. The net result is that a truthful statement will be rich in details, while a false one will be a stripped-down version, lacking details that verify the statement.

A fabricated story tends to be more straight-forward and logical than a truthful one. The statement often shows better emotional control than would be logical to expect, and relates the incidents in a manner that leads to a logical conclusion. Real life is rarely this neat.

Practiced Liars

Some people enjoy deception. These belong to the minority we call "pathological liars." They won't tell the truth without embellishment, or distortion, even when it serves no purpose. These are the types of people who gravitate into certain occupations, such as sales, advertising, public relations, or politics.

They intuitively know that the best way to put across a lie is to tell it forcefully and boldly. They know the "big lie" tech-

nique by heart, and practice it. They won't trip themselves up by weak statements, or playing word games.

These people are very hard to catch in a lie, without outside information. They can look straight in your eye and lie to you, without hesitation and without anxiety. Unless you know, from independently developed information, that their statements are false, you can't tell that they're lying.

Deception

We can learn from the successes of professional liars, and from the errors of those who try to lie, but fail. The main point is to state a lie boldly and confidently, without hesitation and without hedging.

Glossary

Big Lie The technique of telling a lie so bold that it fools the listener because he can't imagine that someone would lie about something so important or basic. The liar may claim to be a doctor, or a millionaire, both of which are easy to check. The victim does not check, because he feels it would be unnecessary.

Closed-ended Question A question allowing only a "yes" or "no" answer, or a very short answer. Examples are: "Were you ever fired?" "Where do you live?"

Confession Admitting to an act. A confession may be true or false. False confessions come about as a result of coercion, or a mental quirk by the confessor. Some people have an urge to confess to sensational crimes, appearing at police stations to

surrender. Others confess under pressure, because of fatigue or simply to stop the discomfort.

Cop-out Slang for a plea bargain.

Copping the Plea Same as "cop-out."

Deal Catch-all term for any agreement for special consideration with an investigator or a prosecutor. This may be a plea-bargain, or an exchange of information for special treatment.

Faking Good Falsification of credentials or answers to make oneself appear better than the facts justify. This term is often employed by people who administer polygraph tests, honesty questionnaires, etc.

Feeding Back An interviewer's repeating a sentence or phrase that the subject has just uttered, and looking at him expectantly, to elicit more details. This is also known as the "mirror" technique.

"Good Guy-Bad Guy" A form of role-playing by a pair of interrogators, in which they whipsaw the suspect by alternating harsh with kind treatment. One interrogator plays the "bad guy," snarling at the suspect and threatening him with dire consequences if he doesn't cooperate. The other provides emotional relief by being kind and considerate, and tactfully asking the suspect to get what he knows off his chest.

Informant Anyone who can provide information to an investigator or police officer. An informant may be a witness to a crime, a victim, or anyone else who has any sort of useful information.

Informer A suspect or convicted criminal who provides information to an investigator in return for special consideration. In practice, many informers volunteer for the task, preferring to inform on a friend or associate than face a criminal charge alone.

Interrogation Questioning of a suspect during a criminal investigation.

Interview Questioning in a non-criminal setting, or of people who are not suspects, e.g., witnesses.

Investigative Key A fact about a crime, which the investigator keeps to himself, as an authenticator in case of a confession. An example might be the type of knife used, something which only someone at the scene would know.

Leading Question Same as "Predicated Question."

Lie Detector Common term for "polygraph."

Mirandize To give a suspect the "Miranda Warning" when placing him under arrest or before beginning a custodial interrogation.

Official Police Police agents working for local, state, or the federal government.

Open-ended Question A type of question designed to give the interviewee the maximum latitude in answering. One such question is: "Tell me about yourself."

Plea Bargain A deal, worked out between the prosecutor and the defendant's attorney, for a reduced charge or sentence in exchange for a guilty plea.

Police We use this term only for police agents of state or local government, and for federal agents. Privately employed officers are "security guards" or "security agents."

Polygraph An instrument to measure and record heart rate, blood pressure, breathing, and skin conductivity, as stress indicators.

Predicated Question A question based upon an assumption, which tends to force a certain type of answer. One such question is: "When were you last fired?"

Pressure Verbal techniques of making the interviewee uncomfortable or anxious. Also includes techniques which have physical effects, such as withholding food, water, tobacco, or permission to go to the toilet.

Private Security Guard A person performing security or guard work for a private agency, unconnected with any government.

Roll Over Slang term for cooperating with the investigator. A suspect may "roll over" on his partner, providing testimony in return for a lesser sentence.

Salami Slicing Enticing admissions from a subject in small increments.

Security Guard Same as "Private Security Guard."

Stonewalling Outright refusal to cooperate. This can take the form of repeated denials, refusal to be interviewed or make any statement, and refusal to answer any questions, even apparently unrelated ones.

Subject A person being interviewed, or under interrogation, who is not necessarily suspected of a crime.

Suspect Any person suspected of having committed, or taken part in, a crime.

Telephone A slang term for an electric-shock machine used for torture. Originally, this was literally a field telephone, with a hand-cranked magneto, used to produce the high-voltage current for eliciting confessions. Today, there are sophisticated plug-in devices built into briefcases, that allow setting the voltage desired, and with an array of clamps and electrodes to fit any part of the body.

Torture Physical techniques of making the interviewee uncomfortable or anxious.

Truth Drug Also known as "Truth serum." Drugs which break down inhibitions and supposedly bring out the truth. Information elicited this way is unreliable, because subjects are suggestible.

Turn Over Same as "roll over."

Voice Stress Analyzer An electronic device to measure and record voice pitch and undertones. This is as unreliable as the polygraph.

For Further Reading

The Book of Lies, M. Hirsch Goldberg, NY, William Morrow and Co., 1990. This is an entertaining, anecdotal book, with a serious underlying tone. It puts the problem of resisting interrogation into perspective, and provides practical pointers on both detecting and practicing deception.

Elementary Field Interrogation, Dirk von Schrader, El Dorado, AR, Delta Press, 1978. This is a textbook of torture, with some attention given to psychological preparation.

A Handbook For Spies, Wolfgang Lotz, NY, Harper & Row, 1980. Wolfgang Lotz has "been there," because he's been arrested and interrogated in Egypt as a spy for Israel. He

had the luck to survive the experience because he was able to pass for German instead of Jewish, and is therefore able to tell what it's like to get the full treatment by the secret police.

Hiring the Best, Martin John Yate, Boston, MA, Bob Adams, Inc., 1988. This is probably the best book on pre-employment interviewing written in America, because it's clear, logical, and complete. Its main value is its focus on the tactics of interviewing, providing practical advice instead of abstruse principles. This book, is, however, misleading in one important aspect. Few employers can afford to hire the "best," and have to be satisfied with those who are willing to work for what they're willing to pay. This is why you're unlikely to find yourself confronted with the slick interviewing techniques explained in this book.

Interrogation, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987. This provides the full picture from the other side of the hill. This manual covers all aspects of interrogation and interviewing, including physical coercion, techno-tactics, personality tests, and other means.

Knock 'em Dead, John Martin Yate, Boston, MA, Bob Adams, Inc., 1987. This book is the mirror image of *Hiring the Best*, cited above, because it's a guide to interviewing from the applicant's point of view. This volume contains Yate's recommended answers to various tough questions and trick questions hiring interviewers are likely to ask.

Lie Detection Manual, Dr. Harold Feldman, Belleville, NJ, Law Enforcement Associates, 1982. This is a standard polygraph manual, which provides the rationale behind the tests, the structuring of questions, and interpretation of the answers. This book gives a good insight into the mind-set of the polygraph "expert," which is useful in coping with a polygraph test.

Notable Crime Investigations, William Bryan Anderson, Editor, Springfield, IL, Charles C. Thomas, Publisher, 1987. This book contains some insights into the techniques of police interrogation. Each chapter is a narrative, and the editor summarizes some investigative tips for the reader at the end.

The Mugging, Morton Hunt, NY, Signet Books, 1972. This book is a detailed account of a mugging in New York, and its aftermath. Its value is the meticulous way it explains how the criminal justice system works, although few systems are as badly overloaded and out of date as New York City's. Pages 95-136 contain a good narrative of the interrogation, as practiced by the hard-boiled New York City detectives assigned to the case.

The Spy Who Got Away, David Wise, NY, Avon Books, 1988. The value of this book is in the detailed description of how the FBI treated Mrs. Howard after her husband defected to Russia. This is an explicit account of how emotional isolation can lead to revealing secrets, if the manipulators are at all clever about it.

Index

- Accusations, 15, 63, 89, 90, 93, 104
Alcohol, 56, 64, 65, 72, 91, 93, 112
Alibi, 41, 155
Ambush interview, 126
Anectine, 78
Answers, 6, 11, 46, 52, 54, 57, 63, 85, 86, 93, 108, 112, 121, 127, 131, 133, 135, 140, 141, 145, 148, 152, 153, 155, 159, 160, 164, 170
Anxiety, 90, 102, 122, 146, 152, 162
Apollo Syndrome, 110
Arrest, 5, 6, 10, 13, 21, 22, 32, 43, 143, 144, 165
Assertiveness, 149
Attorneys, 5, 20, 24, 25, 35, 129, 130, 131, 133, 148
Back-up story, 155
Background check, 26, 87, 88, 114, 115
Barnes, William W., 42
Baseline, 50, 85
Biased Language, 124
Biofeedback, 91
Biting tongue, 92

- Blood pressure, 83, 84, 89, 91, 152, 165
- Body language, 20, 42, 43, 50, 151
- Breathing, 78, 83, 165
- Career criminals, 5, 9, 31, 46, 70
- Carpenter, John, 24, 27
- Cell-mate, 70, 71
- Central Intelligence Agency, 6, 12
- Closed-ended questions, 118, 119, 163
- Coaching, 116
- Coercion, 2, 11, 12, 64, 71, 76, 77, 126, 163, 170
- Conditioning, 49, 50, 51
- Confessions, 11, 13, 14, 15, 25, 41, 42, 44, 60, 75, 99, 101, 103, 163, 165, 166
- Control questions, 85, 86, 87, 91, 92
- Conversational tricks, 41, 55
- Courtroom Testimony, 132
- Covert interrogation, 2, 67, 69, 73
- Covert interrogator, 70
- Covert investigator, 72
- Criminal investigation, 1, 4, 18, 19, 61, 139, 159, 165
- Criminal investigators, 29, 30
- Cross-examination, 132, 133
- Cumberland Farms, 14
- Custodial interrogation, 22
- Damaging admissions, 22, 23, 25, 86, 89
- Damaging information, 18, 38, 70, 111, 114, 157
- Damaging statements, 2
- Deception, 5, 43, 46, 59, 61, 62, 63, 64, 66, 84, 86, 89, 90, 92, 93, 141, 145, 146, 151, 159, 160, 161, 162, 169
- Deceptive tactics, 57, 59, 60, 61
- Demara, Ferdinand, Jr., 107
- Denial of guilt, 93
- Deposition, 36, 129, 130, 131, 132, 133, 135
- Derogatory information, 2, 72, 73, 112, 114
- Desensitization, 122, 152
- Direct examination, 133
- Disarming Candor, 146, 147
- Double-bind, 55
- Drugs, 10, 11, 31, 34, 56, 65, 69, 72, 77, 78, 90, 112, 118, 119, 167
- Elavil, 91
- Electric shocks, 78, 80, 166
- Emotional isolation, 143
- Emotional stress, 85, 89, 146, 160
- Employee Polygraph Protection Act, 87
- Employment agency, 116
- Employment applicants, 34, 87, 89, 114, 115
- Employment application, 26, 109, 111, 112, 148
- Employment application blanks, 112
- Employment history, 122
- Employment interviewers, 40, 55, 114, 117, 149
- Employment interviews, 2, 18, 22, 26, 38
- Employment screening process, 111
- Espionage, 13, 59
- Eye contact, 4, 43, 92, 145
- Fake friend, 70
- Fake informer, 103
- Fake line-up, 61, 62, 141
- Fake prisoner, 71
- Faked ending, 64
- Faking good, 110, 146
- Federal Bureau of Investigation, 3, 12, 25, 30, 60, 70, 171
- Fellow employees, 3, 56, 70, 108
- Field Interrogation, 99
- Fifth Amendment, 21, 22, 54, 139
- Fishing expeditions, 60
- Flattening stress responses, 91
- Fleischman, Gary, 24
- Friendliness, 50, 101
- Fuchs, Klaus, 24, 25, 60
- Gestapo, 76
- Global scoring, 92, 93
- Good guy-bad guy, 51, 154, 155, 164
- Hostile question, 127
- Howard, Edward Lee, 12, 13, 36, 171
- Mary, 12
- Inconsistencies, 3, 52, 116
- Informers, 70, 102, 104, 157, 164
- Innocence, 19, 42, 46, 93
- Insubordination, 23, 56
- Interrogation by Deception, 100
- Interrogations, 4, 6, 9, 14, 18, 35, 49, 50, 52, 80, 139, 143
- Intimidation, 13, 22, 26, 51, 52, 84, 87, 109, 122, 128, 142, 143, 149
- Keeler, Leonarde, 84
- Kinesic interviewing, 20, 43, 45
- Language, 21, 42, 43, 110, 153, 159, 160
- Larson, John A., 83

- Lawyers, 23, 45, 46, 135, 143
- Layered questions, 119, 120
- Lie detector, 20
- Linguistics, 4, 41, 45, 46, 63, 159
- Loaded questions, 41, 53, 55, 64, 149
- Lombroso, Cesare, 83
- Mcfarlane, Robert, 88, 89
- Media interviews, 123, 124, 125, 126, 127, 128
- Military interrogations, 99
- Military interrogators, 33
- Miranda Decision, 21
- Miranda Warning, 11, 20 21, 22, 56, 59, 71, 165
- Miranda, Ernesto, 20, 21
- Morphine, 78
- Nervousness, 43, 46, 90, 92, 142, 146, 151
- Nye, Harold, 39
- Objectivity, 45
- Off the record, 125
- Omissions, 147
- One-word question, 56
- Open-ended, 165
- Open-ended questions, 39, 119
- Paper-and-pencil tests, 33
- Peak of tension test, 86
- Perjury, 31, 133, 134
- Physical coercion, 77, 78
- Physical discomfort, 101
- Poise, 119, 120, 149, 151, 153
- Police officers, 5, 10, 11, 12, 21, 22, 24, 25, 26, 31, 32, 38, 40, 43, 62, 71, 76, 88, 143, 144, 157, 164
- Polygraph, 13, 20, 23, 33, 45, 46, 63, 83, 84, 86, 87, 88, 89, 90, 91, 92, 94, 164, 165, 167, 170
- Post-test interrogation, 63, 86, 93
- POW, 33, 98, 99, 100, 103
- Pre-employment interviews, 107, 122
- Pre-employment screening, 108
- Predicated question, 55, 149
- Pressure, 1, 5, 33, 40, 49, 57, 77, 79, 83, 84, 101, 102, 151, 164, 166
- Private investigators, 3, 4, 22, 38, 40, 43, 56, 71, 72, 89, 142, 157
- Private security officers, 14, 15, 32, 76
- Probable cause, 31
- Psychological coercion, 78
- Psychological tricks, 118

Questionnaire, 63, 87, 112,
135, 164

Reflexive question, 54, 150

Rehearsals, 6, 121, 122, 146,
152

Relaxation exercises, 91, 142,
151

Relevant questions, 85, 86

Rent-a-cops, 32

Resisting interrogation, 6,
139, 140, 145

Rivera, Mike, 13

Routine questions, 50, 52,
85, 131, 132

Salami Slicing, 101

Self-incrimination, 21, 54

Shock Interrogation, 100

Single-word question, 55

Skardon, William, 25

Skilled interrogator, 62, 153

Staring, 56, 140

Statements, 22, 23, 24, 26,
29, 41, 52, 53, 64, 65, 70,
75, 93, 101, 110, 125, 148,
156, 162

Stonewalling, 23, 31, 139,
166

Stress question, 120

Stun gun, 79

Suggestibility, 46, 55, 124,
140, 141, 167

Sworn testimony, 128, 129,
130, 131, 132, 135

Tactics, 6, 19, 20, 22, 26, 33,
37, 51, 59, 67, 99, 101, 102,
139, 143, 154, 160, 170

Thumbtack in shoe, 91

Tinning, Marybeth, 42

Torture, 5, 11, 12, 13, 34, 51,
59, 73, 75, 76, 77, 78, 79,
80, 81, 166, 169

Tranquilizer, 90

Tricks, 52, 60, 64, 84, 87, 92,
104, 124, 144, 149, 154

Truth, 3, 6, 40, 41, 42, 60,
110, 119, 129, 133, 153,
161, 167

Undercover agent, 4, 10, 71,
72

Unskilled interrogator, 153

Unskilled interviewer, 1, 119

Unwilling or uncooperative
subject, 1, 2, 6, 80

Used car salesmen, 46

Valium, 90, 91

Voice stress analyzer, 94

Wannabe, 32

Wannabes, 32

Weaseling language, 93, 160

Wells, Floyd, 70

Wylie-Hoffert murder case, 5

Yate, Martin John, 116

Dirty Tricks Cops Use

(and why they use them)



Bart Rommel

CONTENTS

Introduction	1
1. Image Versus Reality	7
2. Speed Traps	11
3. Handling Suspects	23
4. Search And Seizure	53
5. Informers And Information	63
6. Obtaining Confessions	75
7. Alibi Guns: Uses And Abuses	109
8. Obtaining Evidence	113
9. Manipulating Evidence	117
10. Entrapment	123
11. Pro-Active Enforcement	131
12. Finale	141
13. For Further Reading	143
Index	149

Introduction

The struggle between police officers and offenders is unequal. Criminals have the initiative, and use it to stay one or more steps ahead of the law. In some cases, criminals are beyond the reach of the law because of jurisdictional problems or other technicalities. This is why police need to make the most of every opportunity to obtain arrests and convictions.

Police do not solve most crimes. According to the FBI and other sources, the clearance rates for most crimes are below 50%. The "clearance rate" is the percentage of crimes "cleared" by arrest. It does not necessarily mean that the criminal justice system convicts the suspect, or even that the suspect spends

2 Dirty Tricks Cops Use

any time in prison after conviction. Murder, which once had a clearance rate of between 95% and 98%, now has a clearance rate of about 75%, according to FBI statistics. The burglary clearance rate, never high, has been dropping steadily during recent years, from less than 20% to about 13% today.

Even minor offenses are easy to carry out because the cops can't be everywhere. In fact, they catch only a tiny minority of traffic offenders. Ask yourself how many times you've seen other drivers dangerously violate the speed limit, run a stop sign, or drive in an erratic manner that suggests they were drunk, without being stopped by a cop.

One reason police solve very few crimes is that they remain unaware of them. According to several studies by the National Institute of Justice, people do not report most crimes to the police.

Part of the answer is, of course, better relations with the people police serve. "Community Policing" is one approach, and the final judgment regarding whether this will work or just be another buzz-word is still not available. In any case, this book is not about public relations, crime prevention, Neighborhood Watch, or other "soft" methods that enhance citizen-police cooperation. This is about heavy-duty enforcement against hard-core criminals.

Police officers deal with some very dirty and immoral people, who sometimes appear to have all the advantages because they know how to exploit every Constitutional safeguard to the limit.

This is the heavy-duty aspect of law enforcement. Officers' ingenuity can sometimes make the difference between "making" and "blowing" a case against a street-smart felon.

There are ways to redress the balance. Law officers have to use certain methods that skirt the edge of the law, and at times even cross over into illegality, to do

their jobs against some of the heavy-duty offenders. A clean cut and morally upright police officer soon finds that his Boy Scout mentality doesn't prepare him for encounters with street-smart offenders and sociopaths. To cope effectively, he has to become more flexible.

Criminal investigators have to be smarter and tougher than their adversaries. They have to have strong stomachs, and they must learn to make hard choices. Not every police recruit is suitable for this demanding work, and those with an inflexible Boy Scout mentality are best suited for patrolling parks and guarding school crossings.

Why this book? This is for the new police officer, who won't find this knowledge in any academy class. The small town or rural officer will also find these lessons from big-city departments enlightening. This book is also for the average citizen and taxpayer, to inform him how the police he supports really fight crime. The methods really used by police officers are sometimes as ugly as the crimes they combat. This information is also protection in case he gets caught in a police "sting." The unfortunate part about stings is that they sometimes trap people who otherwise would not be trying to commit illegal acts. Finally, the methods listed here are also adaptable for use by private security agencies, and not necessarily for legitimate law enforcement.

It's unfortunate that some police officers appear to concentrate on apprehending relatively minor offenders, and even innocent citizens, instead of hitting hard at heavy-duty felons. One reason is that it's safer to arrest a yuppie smoking a joint in his BMW than to shoot it out with a heavily-armed drug dealer. Another is the constant pressure for "production," statistics that help the police chief prove that his agency is doing a good job, and deserves a larger budget. A profusion of easy arrests looks better on

4 Dirty Tricks Cops Use

paper than a small but select number of 'quality' arrests.

Despite the best efforts of progressive police administrators, police work is still highly politicized in many jurisdictions. The mayor of one city urges police to hand out more traffic tickets to boost city revenues. The mayor of a small town tells his police chief to enforce the law, but "Don't arrest my cousin."

There are moral judgments to draw regarding police actions. The parallel with the military is close, because the military have to commit immoral acts for a higher purpose. It's their job to kill the enemy and destroy his power to sustain a war, even if this includes bombing his cities where civilians are targets as well as war plants. Bombing cities, done by both sides during World War II, took many innocent lives, including those of women and children. Courageous and dedicated airmen nevertheless carried out the bombings against determined opposition, in the belief that taking enemy lives, even innocent ones, would save the lives of their fighting compatriots on the ground.

Several international agreements forbid atrocities, and regulate the conduct of the military. Many of these are honored in the breach under the pressure of military necessity. Expediency rules that the military will destroy certain civilian targets, although random shooting of civilians occurs less often because it doesn't contribute to the war effort.

The scruples most military follow are to avoid wanton destruction, and not to make a personal profit from the war. Striking at civilian targets not vital to the enemy's war effort is outside the moral code, as are looting and rape. Many military won't condone unnecessary violence against civilians, because they have a strictly defined moral code.

The difference between police and military is that police officers are peace officers, and are not allowed the same freedom as military men. Those who enforce the law are required to follow it to the letter, both by the law and by their superiors.

Some officers use questionable methods to try to do a better job, risking their careers in the service of a higher good. Occasionally, police officers use strictly illegal methods to obtain arrests and convictions. Whether these are justifiable or not is often a gray area. Obviously, it's both legally and morally wrong to shoot a jaywalker, but paying informers with illegal drugs is not as clearly wrong, although it's always technically illegal. Likewise, planting evidence to obtain a conviction of a known long-term career criminal isn't clearly wrong, although it's illegal as hell.

Will this book help criminals? Not really, for two reasons. First is that criminals usually don't read. Instead, they watch TV or video cassettes. The second reason is that, for the criminals who do read, this book provides nothing new. Everything contained in this book was published elsewhere, usually in the daily news reports. Many street smart career criminals have also taken the post-graduate course at what we sometimes call 'the crime college,' the penitentiary.

NOTE: This book uses the masculine pronoun in most discussions, defying the politically correct convention to use "non-sexist" language. This is in recognition of the reality that most police officers, and most criminal suspects, are still male, and that politically correct terminology such as "he/she" or "police person" is awkward to write and to read.

1 Image Versus Reality

Citizens from middle class, affluent, suburban backgrounds may be surprised and dismayed by the harsh reality of the mean streets of crime, and what police officers have to do to obtain convictions. It's not like what they see on TV.

The media have always given prime-time treatment to law enforcement. During the heyday of radio, crime shows such as *The FBI in Peace and War* and *Mr. District Attorney* highlighted and glorified many law enforcement agencies. TV brought new police shows, such as *Dragnet* and *Adam 12*. Joe Friday, the laconic, moralistic, even starchy detective in *Dragnet*, always got his man.

8 Dirty Tricks Cops Use

Most importantly, he solved his cases by going strictly by the book. The two clean-cut, clean living patrol officers in *Adam 12* also fought crime and won, their morally upright Boy Scout demeanors an asset to their operations.

Some Hollywood movies are more true-to-life. *Dirty Harry* is an excellent example. Harry Callahan is a street-smart cop who takes no prisoners, and who is at odds with high departmental officials because of his rough-and-ready methods. The plot and dialog of each *Dirty Harry* film show that police administrators and politicians are more worried about their public image than about the realities of violent crime. Harry himself is a cynical, nasty, thoroughly disillusioned detective who understands that violent criminals understand only one language, that of force. He feels that violent criminals get off on technicalities and go on to victimize other citizens because of the ineffectiveness of the criminal justice system.

His solution to the violent crime problem is crisp and violent. His attitude, shown in the oft-quoted "make my day" scene from *Sudden Impact*, is that terminating a violent criminal on the spot is the only sure cure.

Real-life police officers, whatever their convictions, must keep a much lower profile than Harry Callahan. Even a "righteous" shooting brings an investigation of the officer and his actions, and in many cases an administrative suspension until the investigation has established that he acted correctly. A police officer who would dare to snuff the biggest crime figure in his jurisdiction would find that his superiors would immediately

disown him, and turn him over for prosecution, because of the adverse publicity. Even a beating under questionable circumstances, such as the Rodney King incident, can have massive repercussions and break careers.

The tremendous positive publicity given to police by TV and by Hollywood doesn't quite cut it with many Americans, who understand that the real-life cops are not like the amiable and superbly competent TV cops. Street wisdom holds that "the cops are never there when you need them," a reflection of the police's inability to prevent or cope with many crimes. The increase in reported crimes, headlined in the press each year, suggests that police are less than effective in their duties.

One result is that many crimes never result in reports to the police. Despite the increase in reported crimes, reflected in the FBI's Uniform Crime Reports, the majority of crimes never get reported. The majority of crimes measured by the National Crime Victimization Survey, an independent study conducted by the Bureau of Justice Statistics of the U.S. Department of Justice, were not reported to police. The most highly reported (75%) crime was motor vehicle theft. The least (13.1%) was household larceny where the value of the property stolen was under \$50 00.

Overall, only 38% of all victimizations were reported to the police in 1990. The most common reason (20%) for not reporting a crime was that it was only attempted, and therefore unsuccessful. The next reason (14.7%) was that the victim reported it to another official. The third most

10 Dirty Tricks Cops Use

common reason was lack of proof, in 10.5% of the cases.

Other reasons were that they felt the incident to be too unimportant, (3.6%) or that it was a private or personal matter, in 6.8% of the cases. In other cases, especially in big cities, people feel that reporting crimes is useless, because the police aren't interested (8.0%) or won't catch the perpetrators anyway (3.3%). Indeed, police did not respond to 14% of violent crimes, 33% of thefts, and 23% of household crimes.

One final reason citizens find that police image clashes with what they see on the streets is speed traps. Motorists ticketed for exceeding the limit by a few miles per hour on a straight road on a clear day may well wonder if this is optimal use of police manpower when more serious crimes are happening. Speed traps have traditionally been common in small Southern towns as a way of enriching the town coffers by fleecing Yankee tourists. This era is mostly in the past, but unfortunately, the practice has spread to other than impoverished Southern towns. Now that large cities in all parts of the country are using police speed traps to build up revenue, drivers should be aware of how to protect themselves. We'll take up speed traps in the next chapter.

Notes:

1. *Criminal Victimization in the United States*, 1990, U.S. Department of Justice, Bureau of Justice Statistics, February, 1992 Report NCJ-134126, pp. 100-102.

2

Speed Traps

Let's begin this study by looking at how not to do it. Speed enforcement, an aspect of traffic law enforcement that is technically easy, is a good example of wasted time and effort if the true purposes are to reduce violations and promote traffic safety.

The official "line" is that speed limit enforcement is to promote traffic safety. Actually, there are two basic types of speed enforcement. One is to promote traffic safety by slowing down or apprehending dangerous drivers, not only speeders, and taking extreme cases off the road by suspending or revoking their licenses. The

12 Dirty Tricks Cops Use

other is to raise money for the police agency's parent body, city, county, or state, and this is known euphemistically as "revenue enhancement." The first objective is legitimate law enforcement. The second is abuse of police power, condoned and even encouraged by cities, states, and the court system.

One former state trooper maintains that hypocrisy pervades the system of speed enforcement, because police officers rarely get ticketed, even when on non-emergency business or even while speeding off-duty. Furthermore, in many jurisdictions normal driving speed is above the limit, and anyone driving at or near the posted limit obstructs traffic because other cars begin backing up behind him.¹

Another hypocritical aspect of traffic enforcement is that many officers will extend "professional courtesy" to other police personnel, refraining from writing them tickets because they carry a badge. Chief Robert E. Shaffer, of Clarion, PA, condemns this "professional courtesy" because he points out that it's the moral equivalent of what we'd condemn as corruption in other occupations.²

Selective Enforcement

"Selective enforcement" is designed to enhance safety by taking down the worst offenders. Police officers stop only the worst speeders, such as those exceeding the limit in a school zone, and those weaving in and out of traffic lanes. They also stop those driving in a

way that suggests they're impaired by drugs or alcohol. Selective enforcement involves patrolling stretches of road and intersections with high accident rates, and watching for drivers who speed recklessly, cut off other drivers, change lanes without signaling, run red lights, and commit other acts that lead to accidents. Such enforcement has to be selective because no police agency has the time or manpower to pursue all traffic offenders. Selectivity puts the emphasis on the dangerous drivers, and leaves the minor technical violators alone.

Revenue Enhancement

Revenue enhancement is another matter, and the tactics are very different. Revenue enhancement involves speed traps, and the reason they're called speed traps is that they're designed to catch safe drivers. A speed trap will most likely be on a quiet stretch of straight road with less traffic than main arteries, where drivers normally let their guard down because driving is easy. Speed limit signs may be obstructed by bushes, and the limit itself may change from block to block to catch drivers who don't pay strict attention to signs.

Radar Ins and Outs

A favorite tool for speed cops is radar, because a scientific instrument is intimidating to the suspect and carries more weight in court. This

14 Dirty Tricks Cops Use

is the same reasoning that makes police favor the polygraph, or "lie detector," and the breathalyzer, although neither one is a reliable indicator of what it purports to measure. If it looks scientific, it's more impressive, especially to those who have a deep faith in "science." This is why the radar ambush is in common use. It's hard for a speeder to say that his actual speed was less than shown on the meter. It's also not a defense in court to say that the driver was being reasonable and prudent when the radar showed him exceeding the posted limit.

Normally, the 85% rule applies. This means that the speed limit is at a point where 85% of the drivers drive at that speed or less on that stretch of road. Setting the limit lower results in a great percentage of drivers exceeding it, because they feel comfortable at the higher speed. As we've seen, another trick is to post several speed limit signs on a short stretch, each with a different speed limit, so that missing even one sign leads to a violation. This generates more business for the speed cops.

Speed cops also depend upon psychology, which is why they don't set up traps where motorists drive defensively and are alert. They wait in locales where drivers tend to lapse into "condition white" because hazards are few. If possible, they set up at a point where the posted limit is lower than the speed at which most motorists drive that particular stretch. Sometimes, they have the help of the traffic engineer, who will post an artificially depressed speed limit to help the police.

Another approach to setting up a speed trap is locating the radar set over the crest of a hill. Drivers normally press harder on the gas pedal when climbing a grade, but any driver who doesn't back off the moment he gets over the top risks exceeding the limit as his vehicle picks up speed on the downgrade. Many drivers don't let up on the gas instantly, and speed cops know this, which is why they choose the reverse slope of a hill for a radar trap.

Another reason is that some drivers carry radar detectors. When a radar set is on the other side of a hill, its emissions, which travel in a straight line, do not alert a radar detector in an oncoming car until it's crested the hill and is within range. Then when the detector beeps, it's too late.

Yet another trick is to set up in an area with a lot of electromagnetic traffic, such as an airport. This makes it hard to detect the radar gun among other emissions, such as airport traffic. Airport radar covers the area by scanning, the antenna turning several times a minute, and the momentary pulse picked up by the radar detector sounds much like the pulses of modern radar guns with on-off switches.

The radar gun with a trigger-controlled transmitter is the most dangerous type. The officer aims it at his target and presses the trigger to turn on the transmitter, unlike the early and crude police radars which sat aimed down the road with transmitters continually on and warning anyone with a receiver that they were approaching the beam.

16 Dirty Tricks Cops Use

There are two types of speed measuring devices which do not depend upon radar. One is VASCAR, which has been in use for years. This is merely a time-and-distance measuring device. To use it, the officer selects a stretch of road between two prominent landmarks, and drives the length of the stretch at whatever speed he wishes. He pushes one switch at the first checkpoint, and another at the second. This measures the distance for the VASCAR's computer. Next, he parks where he can see both checkpoints, and when a car approaches, he pushes a "start" button when it crosses the first checkpoint, and the "stop" button at the second. This measures the time the car took to travel the distance, and the VASCAR's computer calculates the speed at which the car was traveling.

The second type uses a laser instead of radar. There are, at the moment, no laser detectors on the market, although this may change any day. The laser beam works just like a radar gun, but it's much tighter and much more directional. Using a laser, the officer can pick out an individual vehicle sandwiched between other vehicles, something radar cannot do reliably. Because lasers are so directional and tight, there's practically no chance of a speeder detecting one from far away, unless it's aimed right at him, in which case he's already in the trap.³

When cops stop someone for a traffic offense, they often ask casually, "Do you know how fast you were going back there?" or "Did you see the speed limit sign?" This isn't casual conversation. The officer tries to get the driver to make an

incriminating statement to be used against him if he decides to plead "not guilty." Admitting guilt can make it much harder in court later, because the cop will record the statement in his notebook. A good answer, without seeming evasive or showing that the driver was not paying attention, is to say that he was watching the road, not the speedometer, because of a potentially dangerous condition ahead.

Quotas and Incentives

Officially, police departments do not have quotas for traffic tickets. However, police officers in Green Bay, Wisconsin, are protesting what they say is a departmental policy mandating disciplinary action against officers who fail to meet a monthly quota.⁴

Unofficial incentives exist. In Arizona, off-duty police officers can earn extra pay by conducting driver improvement classes. Arizona law mandates that for the first violation during each two year period, the driver has the choice of going to court or signing up for a driver improvement class, which at the time of writing costs about \$75. Taking this option keeps the violation from appearing on the driver's record. An added incentive for the first offender is that a recorded violation serves as an excuse for his insurance company to raise his premiums. Clearly, choosing the driver improvement class has benefits, among which are that the officer conducting the class earns extra money.

Coping With Speed Traps

The first and cardinal rule is to remain alert for ambushes and situations that may contain them. This seems like very elementary advice, but it's surprising how many people drive while paying only casual attention to their situations. 'Situational Awareness' is the basis both for safe driving and avoiding speed traps.

Extra vigilance when rounding a bend in the road or topping the crest of a hill is important, because speed cops rely on surprise. A curve or down-slope can easily conceal a speed cop and his electronic device. Another favorite spot is in the shadow cast by a bridge or retaining wall.

For the many motorists who end up stopped by a speed cop, there's a right way and there are many wrong ways to prepare. A basic step is to look 'clean,' because first impressions are the most important ones. Police officers tend to treat with respect, or at least civility, the driver who appears neatly groomed and well-dressed, and who drives a clean car. A driver who hasn't shaved for a week, wears torn and dirty clothing, and generally fits the image of 'dirtbag' is in for a rough time, especially if the seats and floor of his vehicle are littered with beer cans and other debris.

A clean appearance and polite manner radiate self-confidence, which is very important. This shows the officer that the driver isn't likely to be a suspect wanted for an offense in another jurisdiction, and raises the slight nagging doubt that the driver may be able to "fix" the ticket through

political connections. It also may move the officer to give the driver the benefit of the doubt, and release him with a warning.

Many people increase their chances of getting a ticket by their demeanor. The worst ways to react to a traffic stop are:

- Be abusive or disrespectful. Insulting an officer will almost always lead to a ticket, or worse. In some rural jurisdictions, there may even be violence, inflicted while the offender is "resisting arrest."
- Claiming to know the officer's superior, or the judge, also doesn't work, because the person who really does has no need to try to negotiate his way out of a ticket with Officer Friendly. A quick phone call later can get the ticket fixed, and that's that
- Threatening to plead not guilty and to 'see you in court ' This will only cause the officer to take extensive notes on the driver, vehicle, nature of the offense, and anything else that may be required during court testimony.⁵
- Hand the officer a fifty-dollar bill folded with the drivers license. At one time, this did work in some jurisdictions, such as New York City, but today many officers are too proud to accept bribes, especially such small ones, and will arrest anyone offering a bribe.
- Accusing the officer of racism, if the driver is a minority group member.

Talking the officer out of writing the ticket takes skill and luck. Drivers stopped for traffic offenses have only one window of opportunity, before the officer begins to write the ticket. The

20 Dirty Tricks Cops Use

driver will make it or break it right then, while reaching for his license and registration. There are many ploys drivers use to try to talk the officer out of giving them a speeding ticket. One, described by retired Sergeant James Eagan, is the "potty ploy."® The driver asks the officer to hurry up with the ticket so that he may proceed to the next rest area to relieve himself. If there are bushes or trees nearby, another variant is possible. The driver leaves the car hurriedly and explains to the officer that he's got to attend an urgent call of nature. Few officers will follow a driver into the bushes to verify that he really had to go.

Another is for the driver to tell the officer directly that he depends upon his vehicle to earn his living, and that he already has enough points so that his license will be revoked or suspended with the next ticket. This appeal has to be delivered with a very sorrowful manner, or it won't work. The officer may write a ticket for a lesser offense, or release the driver with a warning. But any attempt to blame the officer, such as suggesting that he'll be responsible for the driver's family starving, will backfire.

There is an excellent book that meticulously covers tactics for avoiding speeding tickets. This is *A Speeder's Guide to Avoiding Tickets*, listed in the further reading section at the end of this book.

Notes:

1. *A Speeder's Guide to Avoiding Tickets*, Sgt. James M. Eagan, N.Y.S.P. (Ret.), NY, Avon Books, 1990, pp. 1-7.
2. *Law and Order*, August, 1992, p. 101.
3. *Law Enforcement News*, NY, John Jay College of Criminal Justice, Oct. 31, 1991, p. 7.
4. *Law Enforcement News*, March 15, 1991, p. 7.
5. *A Speeder's Guide to Avoiding Tickets*, pp. 27-28.
6. *Ibid.*, pp. 46-48.
7. Author's personal experience.

3

Handling Suspects

A danger police officers face is that the next public contact may be dangerous and assaultive. An officer who stops a car for a broken tail-light may find that the driver is a bank robber who mistakenly thinks the officer is about to arrest him for a felony and opens fire. Although this rarely happens, officers have to act on the possibility that any public contact may become violent.

Nonverbal Cues

Street law enforcement is not like TV. Officers depend on situational, verbal, and behavioral

cues for early warning of dangerous situations. Hunches rarely play a part in real life, mainly because tangible indicators are often present, and officers don't need to rely on intuition. The most obvious cases are "felony in progress" calls, and serving arrest warrants.

A person's ethnicity or apparent economic status may offer cues. This is why some police practice appears classist or racist, but is actually the result of strictly empirical street wisdom.

A black man walking or driving in a "fily-white" neighborhood is much more likely to find an officer stopping and questioning him than a Caucasian, unless he appears to have legitimate business there. A black dressed in a postal uniform, or driving a delivery truck, appears innocuous because he fits in and is unlikely to be stopped for questioning.

A shabbily-dressed person is more likely to be the object of a field interrogation than someone dressed like a bank president. This is the result of the practical observation that bank presidents don't pick up gas stations or commit burglaries. Another practical reason is that the well-dressed person is more likely to have connections "downtown," and may be able to generate heat for any patrolman who stops him without justification. This is very important in agencies in which politics plays a major role.

Race also is a factor because of crime patterns. The U.S. Census shows that blacks comprise less than 13% of the U.S. population, yet FBI Uniform Crime Reports show that 60% of the murders reported are committed by blacks. Similar dis-

proportions apply to other street crimes. A New York State study by the Correctional Association of New York and the Coalition for Criminal Justice found that on a typical day about 23 percent of blacks between the ages of 20 and 29 are under the control of the criminal justice system — in prison, or on probation or parole. The corresponding rate for Hispanics is 12%, and for Caucasians, 2.7%.

This does not mean that blacks are congenitally criminal, but simply that they are over-represented in street crime. Caucasians appear to be very prominent in white-collar crimes, such as high level stock frauds and embezzlements, but these are not within the jurisdiction of patrol officers.

At times, police face a dilemma in ghetto areas. However, when they do, the residents may interpret this as "leaning" on them. This is especially true because crime is usually intra racial, and police seek their suspects among ghetto residents.

In traffic stops, the officer routinely runs a check on the driver's license and vehicle registration. This usually includes a check for warrants, to determine if the driver and vehicle have any warrants or alerts out on them. Sometimes, this check comes back positive, and it's then necessary to arrest the person. It's simply not good police tactics to attempt an arrest alone, especially if the suspect appears to be a physical match for the officer or has a record of resisting arrest. If the situation appears dangerous, the officer will ask for a back-up to assist him, and

26 Dirty Tricks Cops Use

play for time while waiting for his back up to arrive.

Establishing and Maintaining Control

A police officer who wants to enforce the laws finds that his approach must vary with the type of citizen he contacts. It's one thing to write a traffic ticket for a grandmotherly type; it's another matter to stop and question a street-smart felony suspect. The officer can afford to treat the grandmother with kindness, consideration, and show profound respect. The brutal rules of the street require another approach with felony suspects, who often have a street-fighter mentality.

The street-fighter mentality is alien to many people accustomed to treating their fellow man with politeness and consideration. To the street-fighter, kindness is a sign of weakness, and he'll react to kindness by trying to exploit it. The street-savvy officer knows that, with this type of suspect, even if the suspected offense is trivial, it's imperative to establish and maintain absolute control of the situation by making it clear that he is "the man." This means conveying to the suspect that he intends to take whatever steps necessary to enforce the law, and that he demands respect.

In Los Angeles, a city with severe crime problems, one of the cardinal sins for a citizen is to show "contempt of cop": Anyone who "disses" (shows disrespect to) a police officer risks some form of street justice. The underlying reason is not just cops' egos. If a police officer allows a person to treat him with contempt this is the

beginning of losing control of the situation, because the suspect will keep pushing to see how far he can go.

The initial approach sets the tone of the situation. When stopping a well-dressed gentleman for a traffic offense, the officer may address him as "sir" and ask politely for his license and registration. The initial encounter with a scruffy suspect wearing gang colors and a prison tattoo is another matter. If the suspect asks, "Who, me?" the officer will say, "Yeah, I'm talking to you, asshole." Only by displaying a tough, no-nonsense, and even brutal, attitude, can the officer control certain encounters with dangerous suspects.

At times, suspects may actually be guilty but evidence is thin or not apparent to the officer. To avoid suspects' getting the impression that they got away with something when the officer finally has to let them go, the officer can do something to make their lives miserable. One tactic in car stops is to surreptitiously spray Mace into the dashboard and air conditioner vents. When the suspect resumes his interrupted journey, he'll get a healthy dose of tear gas.³

A variation on this theme works especially well when the car has fleece seat covers, or at least cloth seats. Spraying Mace into the fleece or fabric produces a long-lasting effect, because body heat causes the active ingredient, chloroacetophenone, to vaporize and irritate the suspect's bottom and crotch. CN, as chloroacetophenone is called for short, produces a long-

28 **Dirty Tricks Cops Use**

lasting burning sensation, and is very hard to remove from the seat.

Finding Fugitives

Normally, it's not necessary to use such elaborate ruses to corral a fugitive. A standard procedure is to locate the suspect first, then decide upon the best way to apprehend him or her. We have to remember that many outstanding warrants are not for armed and dangerous fugitives, but for traffic scofflaws, fathers delinquent in child support payments, and other miscellaneous, non-violent crimes. Many people with outstanding warrants don't make a determined effort to evade the law, hoping only that it won't catch up with them.

A basic step is to interview the suspect's landlord and/or neighbors to determine if anyone can provide a forwarding address. Another step is to send him a registered letter, with a "show address where delivered" tag. In cities with city-owned utility companies, it may be possible to trace a suspect by the latest address listed with the utility department. However, some apartments offer utilities included in the rent, and renters' names never appear on any utility bill.

Yet another way to trace a wanted person is by canvassing his relatives and known associates. Some will feel obligated to cooperate with the police, and will provide his whereabouts.⁴

At times, officers have one or more likely addresses for the fugitive, but have trouble laying

hands on him. Arresting a fugitive requires that officers and suspect be at the same place at the same time, and their movements often don't coincide. An example is the wanted person who holds a job, and sleeps at his parents' home. The simple way of making contact is to pick a time after the fugitive comes home from work.

When there's more than one possible address, the arresting officers must try to locate the suspect's current location. The telephone can be very useful. A few calls may pinpoint the suspect. Simply asking to speak with him will disclose whether he's at a particular place.

Street-smart suspects move around a lot, and evade surveillance by making their movements unpredictable. One way of coping with this tactic is for the officer to telephone the suspect's home and leave a message to call him on a pager number "Hey, this is Mike. Have Jackie call me at 123-4567." Some officers use an additional ruse to motivate the suspect into returning the call, stating that they owe the suspect money and would like to pay him back.

The pager serves as a "cut-out," a way of making contact without revealing the officer's true identity or location, which might be around the corner from the suspect's address. Officers with cellular phones can place calls while keeping the premises under observation. The pager displays the number where the officer may return the call, and if this number corresponds to one of the suspect's known locations, it pinpoints him. If the officer is nearby, he can be there in a minute.

30 Dirty Tricks Cops Use

If none of these methods work, it still may be possible to trace an individual through his employment. Although a particular person may no longer be at the employer listed on police and court paperwork, canvassing employers in the same field can be productive. This isn't as complicated as it might seem. Restaurant workers, for example, have only a manageable number of employment possibilities in all but the largest cities. Telephoning restaurants may disclose the suspect's location if the officer knows that the suspect is working under his own name, or knows his alias. If not, canvassing restaurants is necessary.

Moving Surveillance

In some cases, it's necessary to shadow a suspect, a suspect's relative, or an associate, to find the target. A suspect may lead investigators to other wanted suspects. Crafty officers must use a variety of tricks to keep the target from knowing he's being shadowed. The most important one is "breaking the profile," changing superficial appearance by donning or removing a coat or hat. This is vital when circumstances force an officer to shadow a suspect without back-up. An excellent portrayal of this technique is in the film *The French Connection*, in which Gene Hackman follows a suspect through the streets and subways of New York. The depiction is so realistic that *The French Connection* is a good training film on this and other aspects of surveil-

lance. The opening scene, showing a detective dressed as Santa Claus, is also true to life.

With a surveillance team, a variety of disguises and ruses becomes possible. Rotating the lead man in a close tail is standard, to minimize the danger of a suspect's "making" him. A stockpile of work clothing and uniforms helps shadowers blend in with the locale. Dressed as postal workers, telephone company employees, and in season, Santa Claus, shadowers can shadow or stake out a suspect while appearing to be part of the milieu.

Conducting vehicle surveillance at night can be very difficult, especially in a heavily-traveled locale, because the suspect vehicle's tail lights blend in with those of other vehicles. Agencies large enough to afford one of the electronic "bugs" that officers can attach to the target vehicle can easily follow a suspect, but smaller agencies don't have all the luxuries and must depend on traditional methods. One cheap and dirty way of making the target vehicle's tail light pattern distinctive is to break one. Keeping track of a vehicle with only one tail light is easier, and trailing officers can hang back to prevent being "made" by the suspect without fear of losing him.

Arrest Tactics

Arresting felony suspects can be both difficult and dangerous. Although the technique of surrounding a house with armed officers and ordering the suspect out via a bullhorn is dramatic, it belongs in Hollywood, and not in real life. Police

32 Dirty Tricks Cops Use

officers prefer to make arrests without violence, if possible, because once violence starts, it can escalate very quickly.

Avoiding injury while making an arrest is important to the officer, who logically wants to go home safely at the end of his shift. This is why the element of surprise is a vital part of many arrests. To attain surprise, it's often necessary to use deception.

In felony warrant arrests, taking the suspect out of his home or stronghold, or out of a crowded room is the first step. There are many ploys to trick suspects into leaving their lairs. One officer, serving an arrest warrant on a suspect attending class in a trade school, had the school administrator send a message to the suspect to come to the office for a long-distance phone call. When the suspect came out of the classroom door, the officer and his partner were waiting on either side, and wrestled the suspect down to the floor and handcuffed him before he could resist.

Sometimes, capturing a suspect alive is the highest priority, even at the risk of officers' lives, because of the information they may obtain from him. FBI agents arresting John Walker, the traitor who handed over U.S. Navy cryptographic materials to the Soviets, knew that he had a lot of information pertaining to the materials he'd passed to the Soviets during his twenty-year career as a traitor. Finding out exactly what he'd revealed to his contacts would enable the government to assess the damage he'd done, which is why the FBI had determined that they needed him alive.

Walker had rented a room at the Ramada Inn in Rockville, Maryland. The previous afternoon, he had attempted to leave material for his Soviet contact at a dead drop nearby. To arrest him, FBI agents decided to trick him out of his hotel room. An agent, William Wang, posing as the desk clerk telephoned his room shortly after three A.M. to tell him his new van had been hit by a drunk in the parking lot. Agents Robert W. Hunter and James Kolouch, wearing body armor, waited for him in the hallway. When Walker emerged from his room, he was carrying a small revolver, and he became suspicious of the two men who were standing by the elevator at that early hour. He drew his gun, and after a short face-down with the agents, obeyed their order to surrender.⁵

Special arrest teams have other ways to get suspects to open the door, and even come out to talk to them. One is the "pizza man" trick, in which an officer knocks on the door and says he has a pizza for the suspect. If there's more than one person on the premises, the one answering the door may think someone else ordered the pizza.

One special anti-crime unit developed other techniques. One was to ring the suspect's bell and ask him if he was willing to sell a boat in his driveway. This lured the suspect out of his house to where officers could put their hands on him.⁶

Another trick to stop and apprehend a felony suspect driving in a vehicle is to have a marked unit make what appears to be a traffic stop. Once the suspect stops his vehicle, officers will either

34 Dirty Tricks Cops Use

get him to leave his car on a pretext, or come up on both sides of his vehicle with guns drawn.

Fugitive detail officers can be very imaginative in luring suspects to where they can make mass arrests. In Corunna, Michigan, a fake wedding was set up by several police agencies to lure drug dealers to where they could be arrested. The fake bride and groom played roles as organized crime figures, and another officer played the clergyman. Several officers were the band, which played at the reception.

Preparations were elaborate. There were even matchbooks engraved with the names of the bride and groom. Police rented a hall for the September 21, 1990 affair, and invited suspected drug dealers. At the door, ushers asked the guests to check their weapons. At a signal, police officers arrested the guests.⁷

Bending The Rules

In certain cases, officers technically neglect their duty when common sense tells them that discretion is the wiser course. The principle of 'discretionary justice' is traditional among police, and it has a sound basis in "street smarts." An example is the officer who stopped two men in a high-crime neighborhood and ordered them to lean against a wall for a search. One of the men told the officer that he had a knife in his pocket before the officer began searching him. The officer took the knife, and told the man he intended to confiscate it, because it was a concealed weapon. Under the law, he could have

made an arrest on that charge, but the cop felt that confiscation solved the problem. The man, however, told him that he carried the knife for protection, because of the high crime threat. He added that he would continue to carry a weapon, because the alternative was to be confined to his home. The officer, upon hearing this, shrugged and gave back the knife.⁸

Police do not arrest suspects at every opportunity. They allow certain illegal activities to continue because those conducting them provide help and information they need. Any experienced beat cop knows that prostitutes often know more about what's really happening on the beat than the officer, and he milks them for information. Allowing the hookers to ply their trade, at least until businessmen and church groups complain, is mutually beneficial. So is tolerating other illegal enterprises. Although technically illegal, certain activities are far less harmful than others. To a street cop, it makes sense to assign priorities, and milk an illegal source for information regarding far more dangerous criminals. We'll study this in the chapter on informers. Philadelphia police allowed a gypsy cab operation to continue because the drivers gave them "tips."⁹

Another tactic works to keep an arrested suspect from contact with his attorney, family, and associates by shifting him from one holding tank or station house to another.¹⁰ An attorney with an order of habeas corpus can't serve it until he physically locates his client. A police agency with many police stations can move the suspect irregularly from one to another, eluding the

36 Dirty Tricks Cops Use

attorney. Small-agency officers can do the same thing by moving a suspect to the next town, or to the county sheriff's jail, making the rounds for as long as it takes to make the suspect feel isolated and to elicit a confession.

Fugitives in foreign countries are recoverable only by extradition, but this is merely the law, not actual practice, in some cases. When there exist good relations between American police officers and those in another country, it's possible to waive the rules and short-circuit the laborious extradition process. American and Mexican authorities have co-operated closely in certain cases. When Morton Sobell, a member of the Rosenberg spy ring, took himself and his family over the border to Mexico in 1950, the FBI took steps to recover him. On August 16, 1950, Mexican security police arrested him as an undesirable alien. Sobell did not go willingly, and officers struck him on the head before bundling him into their car. Another squad of officers gathered up Sobell's family and their luggage, and police drove them to the border at Laredo, Texas, in a convoy. At the border, Mexican police simply told them to walk across to where FBI agents were waiting.¹¹

Federal agents aren't the only ones to obtain cooperation from Mexican police. California police agencies have also made use of the Mexican police's method of *de tacto* extradition, which avoids formalities such as warrants, courts, and lawyers. Mexican officers simply take custody of the fugitive and transport him to the

border crossing where American officers will be waiting. Then they simply release him and order him to walk north.¹²

Arranging such an informal deportation in a manner convenient to both police agencies requires finesse and diplomacy. Mexican officers, like cops throughout the world, are sensitive about protocol on their own turf, and any foreign police officer must remember that he's only in a position to request cooperation, not to give orders. An officer who enters Mexico and begins to behave like "big daddy" will cause his welcome to sour. One Los Angeles Police lieutenant didn't realize this when he went south of the border to handle a transaction that he would have been better off leaving to subordinates. When he became pushy, Mexican officers simply took the handcuffs off their prisoner and told the lieutenant he could do what he wished with him. The lieutenant stuffed the fugitive into the trunk of his car and made for the border without a police escort, leaving some physical evidence behind. Once on American soil, a charge of violation of civil rights by his prisoner became possible, and other officers had to get their stories straight to forestall such a move.¹³

Departmental Policies

During emotional moments in pursuit of their duties, police officers sometimes exceed their instructions, exceed departmental policies, and even infringe the penal code. One common type of incident relates to suspects who resist arrest,

38 Dirty Tricks Cops Use

and who injure police officers in the process. Once in custody, it's 'pay-back time.' Either in the patrol car, or in the police station, the suspect may suffer injuries that will go on the report as having been incurred while 'resisting arrest.'

When several California officers beat Rodney King with their nightsticks on March 3, 1991, and an amateur videocamera operator caught it on tape, it was headline news for days. The trial, and the riots that took place in Los Angeles after the 'not guilty' verdicts, kept the case in the headlines for over a year.

TV networks had originally released a carefully manicured version of the tape, edited to make the incident appear worse for the officers than it was. Indeed, this version of the tape played on national networks and local channels repeatedly, convincing many viewers that the officers were guilty without doubt. However, this was not the first such incident. In Kansas City, Missouri, police officers arrested James Sevart, Jr., after an hour-long pursuit. Sevart had fled when officers wanted to question him regarding a burglary. A local TV news crew video-taped the arrest, and the tape showed several officers holding Sevart down, while an officer struck him at least three times with an object and another officer kicked him.¹¹

Even the Rodney King incident served a constructive purpose. While Los Angeles Police Chief Daryl F. Gates maintained that this was not typical, another police chief thought it important enough to use as training material. William Rathburn, a former LAPD Commander and the

new Chief of the Dallas, Texas, Police Department, uses the videotape of the King beating as a training vehicle. His officers watch the tape and discuss the issues involved. Rathburn intends that no such incident will ever happen in Dallas.¹⁵

With all that, some officers continued to pummel civilians in front of video cameras. California Highway Patrolmen Reginald Redmond and Nicholas Chouprov received suspensions without pay for beating two Persian Gulf war protesters at an otherwise non-violent rally in January, 1991.¹⁶

In Huntsville, Alabama, a local TV station presented a videotape that allegedly showed a city police officer using excessive force on a suspect. The department suspended the officer with pay pending investigation.¹⁷

In Fort Worth, Texas, an officer who was videotaped beating a handcuffed suspect lost his job. However, a grand jury had knocked down assault charges against the officer, and the officer's lawyer said that he intends to appeal the department's action.¹⁸

At times, what first appears to be excessive force is justified. Police officers in Oregon shot a suspected drug dealer 28 times. The suspect had pointed an empty gun at them, but a grand jury ruled that the officers had no way of knowing the gun was empty, and that the shooting was justified.¹⁹

It's a mistake to use excessive force because of emotion, because such an incident can break an otherwise promising career. On the other hand,

selective extra-legal application of force can serve good ends when lesser methods fail. This is what we call "curbstone justice."

Curbstone Justice: Short-cut Law Enforcement

This is summary punishment on the street, completely unofficial and without paperwork of any sort. After the incident is over, it's closed by mutual agreement. A police officer may administer a beating to a man disturbing the peace, instead of arresting and charging him. Some instances of 'curbstone justice' cover more serious crimes. 'Curbstone justice' or "street justice" is a traditional and time-honored method of informal law enforcement.

Often, cops hand out summary beatings to juveniles, perhaps compensating for the discipline they feel they did not get at home. One incident occurred shortly after World War I, when beat cops regularly worked foot patrol. A boy, riding as passenger in a stolen car, was stopped by the beat cop. This officer knew everyone in the neighborhood, including the boy and his family. Instead of arresting the boy, the beat cop slapped him hard across the buttocks with his nightstick and said, "Get the fuck outta here, ya little bastard, before I tell your father."²⁰ In this situation, the father's authority was more to be feared than the criminal justice system.

Several Philadelphia officers, after a report that a young girl had been molested by a suspect they knew, picked him up and brought him to

the station. Several members of the squad pummeled him with nightsticks until he fouled himself, literally beating the shit out of him. They then took him downtown. The suspect did not file any charges against the officers, conceding that he'd gotten what he'd deserved.²¹

Sometimes curbstome justice serves as a deterrent when no other method, such as a restraining order, works effectively. One New York City detective of the pre-WWII era, "Broadway Johnny" Broderick, and his partner, Johnny Cordes, repeatedly got into altercations with suspects and became legends in their own time. A typical incident would begin as members of a "protection racket" gang tried to extort payments from a shopkeeper. A complaint to the police would bring about the arrest of the suspects, but later friends of the suspects would visit the shopkeeper and inform him that, if he pursued the complaint, he wouldn't live to testify at the trial. Broadway Johnny would confront the thugs who had made the threat and administer a beating, telling them that if they threatened the complainant again, he knew where to find them. This "hand talk" was much more effective than any injunction issued by a court. On the street, naked force gets suspects' attention much more than does a piece of paper.

A principle some officers follow is to dispense street justice to "rabbits," those who flee when ordered to stop. Quick administration of summary justice serves as a deterrent.²²

At times, subtle methods of street justice serve to harass a lawbreaker. One method is to

42 Dirty Tricks Cops Use

telephone a suspect's wife and tell her that her husband is having an affair. This method is more effective if a woman places the call. In other cases, planting physical evidence for the wife to find bolsters the accusation. A condom or women's panties on the back seat of the husband's car will convince all but the most trusting wife, and a phone call will ensure that she finds it.²³

Some underworld figures obtain legitimate employment as a cover for their real activities. When this happens, one tactic is for an investigator to visit his employer and ask if the suspect works there, then leak that he's under investigation for organized-crime connections.²⁴

Coping With Electronic Media

Police have always had problems with certain elements of the media. Inevitably, there are a few cop-haters who always interpret police actions in a negative light. If crime is on the rise, it's the fault of the police, even though the police are not the ones who commit the crimes. If police officers take any short-cuts in pursuing a case, these media people criticize them for using excessive force, or abuse of authority. Although it's obvious that you can't make an omelet without breaking eggs, police officers have to be magicians who can do exactly that, by their standards.

Conventional news reporting is dangerous enough when the reporter or his editor is a cop-hater. Electronic media can be worse, because

video cameras can document a mis statement by a police officer, using his own words or actions to fortify a media trial, convicting the officer on the six o'clock news.

The point for officers to note is that it's important to be very careful when using force, and to be mindful of the possibility that a camera may be recording the action. Using force outdoors or in any public place exposes the officer to the danger of an electronic witness recording his actions. The greater danger is that a news program director, in the race for higher ratings, may edit the tape to show the officer in the worst possible light, as happened in the Rodney King incident.

If it becomes necessary to use force on a suspect, an indoor setting is more secure because of limited access. Even a telephoto lens can't see through a wall.

The type of force is important, as well, because of visual impact. A videotape of an officer striking a suspect with a baton has tremendous visual and dramatic effect. This is true regardless of justification. A suspect who resists arrest and fights the officer can be made to appear as if he's merely defending himself against police brutality. By contrast, a shooting takes very little time, much less physical exertion, and doesn't appear as dramatic because there's less action.

Chemical agents are safe and effective. Overpowering a belligerent suspect with "Bodyguard" and similar aerosols is quick and not visually exciting. Obviously, there's no blood for color

44 Dirty Tricks Cops Use

cameras to record, and although the suspect may feel as much physical pain from the effects of the pepper spray as from a baton, the scene doesn't appear as dramatic and sensational. This is very important for the officer working in an area where the media are hostile to police.

A valid justification for use of force is when the suspect assaults the officer. Of course, many suspects will submit to interrogation and search on the street, especially when outnumbered by police, and it becomes more difficult for the officer when there are witnesses or video cameras. There are, however, several ways of inconspicuously inducing a suspect to attack and justify the officer's use of force. One officer kept a pin in his Sam Browne belt, and would jab the suspect during a search. Another is to produce pain by jabbing the body's sensitive areas, such as the testicles or a tender spot in the armpit. Flicking a finger into someone's eye also will stimulate him to attack the officer. The officer blocks the view of witnesses by getting in close to the suspect. This works very well on a suspect driving a car, and it's possible to flick a finger quickly into his eye without passengers seeing it.²⁶

The Ultimate Sanction: Execution

Summary execution of suspects is another topic on which sketchy information exists. Fictional cops such as Dirty Harry Callahan do it all the time, perhaps because Dirty Harry never has to face an officer-involved shooting

investigation team, nor has to fill out the paperwork a killing requires. It's not an exaggeration to say that a shooting takes three seconds, and the subsequent paperwork takes three days.

Among cops, there's a lot of locker-room talk along the lines of "blow them away," the casually stated determination that the suspect's life is cheaper than dirt. Reality is different, because the consequences of an illegal shooting can be severe, involving both criminal and civil litigation.

As many officer-involved shootings take place in locales without witnesses, the only account of the events is the officer's. Without contradictory physical evidence, there's no way to dispute the officer's account. Planned street execution of a known criminal is a dangerous undertaking, but much easier for police than for private citizens because police know the subtleties of escaping detection. Leaving the scene after the execution is one way of avoiding official involvement.

The typical target for street execution is a very dangerous suspect, such as a cop-killer or organized-crime figure, who has frustrated previous efforts to obtain enough evidence to sustain prosecution. Organized-crime operators are especially difficult to prosecute because they're very street smart and take precautions to use cut-outs who protect them from direct involvement.

There are several reasons for street executions of special suspects:

1. Execution can be in lieu of arrest and prosecution when solid evidence is unavailable.

46 Dirty Tricks Cops Use

2. Execution can prevent the suspect from continuing his criminal career and committing more crimes.
3. Execution can be an effective conclusion to a case that's inexpedient to prosecute even when enough evidence is available, such as one involving national security. One such instance, involving a double agent, was too awkward to prosecute, and violent termination was the best choice.²⁶
4. Execution can serve as a deterrent, a warning to others in the same criminal enterprise. Execution is far more effective than a verbal warning to "Be out of town by sundown." The warning can be overt, such as the suspect's body left in a public place, or it can be more subtle, as in the case of a mysterious disappearance.
5. Finally, execution can be defensive. Some suspects are so dangerous that, if they threaten to "get" an officer or his family, it's imperative to take the threat seriously. Drug dealers, biker gang members, and a few others have assaulted and even killed police officers gratuitously, or for revenge. The shooting of Patrolman Byrne in Queens, New York, on February 26, 1988, was an execution with a head shot from a .38-caliber handgun. The killer had no substantial motive: he did it just for the thrill.

Execution of suspects can be "ad hoc" or systematic. A police officer holding a suspect may decide to "cancel his ticket" on the spot if no witnesses are present. Another way is a planned

and informal action by two or more officers working together to ensure "back-up."

One peculiar incident of excessive zeal ended in death for a transient. The police chief of Clay, West Virginia, allegedly spiked wine bottles with castor oil in an effort to rid the town center of drunks. The chief had told others about his tactic of spiking wine, so that the word would spread to the winos and deter them from loitering in the center of town. One drunk, though, died of pneumonia three weeks after drinking wine allegedly spiked with castor oil. The Chief, facing an attempted murder charge, is free on bail, partly because he's the only law enforcement officer in town.²⁷

Finally, there is the unofficial "special squad," operated in secret by a police agency. The Federal Bureau of Investigation did operate a totally secret squad apart from its regular roster, composed of agents who undertook special dirty jobs for the Bureau. These were completely unofficial, working outside normal Bureau channels.²⁸

Organizing such a special squad requires special recruitment methods. A special squad operator is not a civil servant, and the squad does not place public advertisements for members. The process is always by word of mouth, with potential recruits available among military veterans, intelligence agency operatives, and even organized crime.

Paying a corps of extra-legal agents both salaries and expenses takes creative book-keeping. Police agencies have slush funds to

48 Dirty Tricks Cops Use

cover expenses and payments to informers, designed to provide untraceable money. The FBI paid at least one unofficial executioner by falsifying his military records, listing him as a "wounded veteran," to provide him with a disability payment for the rest of his life.²⁹

Tactical planning can be elaborate or simple. Police officers setting out to execute a suspect run the operation somewhat like a raid without the benefit of a search warrant. Goals are to accomplish the task and to avoid detection. Avoiding detection isn't as easy as it seems, because a badge isn't necessarily an asset. Many police agencies have their "Dudley Dorights," set upon furthering their careers by "burning" other officers, and encountering one of these can blow the plan sky-high and result in an indictment for murder.

The elements of a successful execution are:

- Proper identification of the target. Executing the wrong person is an intolerable error. Apart from taking an innocent life, a mistaken hit can cause an international incident. When Israeli hit men assassinated a Moroccan waiter they thought was a terrorist in Lillehammer, Norway, repercussions were severe.³⁰
- Deciding upon a time and place where the target is unprotected or most vulnerable. This can be extremely difficult if the target has a large retinue and is always accompanied by bodyguards. Ordinarily, a simple ambush along the target's normal travel route or an attack at his home, will do the trick. In some cases, it's more desirable to set him up, luring

him to a certain place on a pretext, and disposing of him there or en route.

- Deciding on the method of termination. Firearms are the best choices, except in situations where noise precludes their use, or when it's desirable to make the death appear "accidental." Since most terminations are surprise assaults, the best way to assure results is firing multiple shots into the target. Depending on a single shot to the head or spine is too uncertain because people have survived such wounds. Firing a single fatal shot depends on good marksmanship, often in adverse conditions, such as darkness. This is especially true if the firearm is a handgun, because handguns are low-powered weapons, lacking the destructive power of rifles and shotguns. Power is sacrificed to make handguns light and concealable. Multiple shots, aimed at several vital areas, offer a better prospect of shutting down the body's systems quickly and permanently.
- Disposal of the corpse. In an overt execution, leaving the body for others to discover is relatively simple. If the target is a gang member, a ready assumption is that he was killed by rivals. In covert actions, it may be necessary to bury, cremate, or otherwise dispose of the cadaver. Burial can leave embarrassing remnants if the clandestine grave later becomes the site of a freeway or building. Another way is to have an arrangement with an undertaker, who can pack an extra corpse into a coffin. Once buried in the

50 Dirty Tricks Cops Use

cemetery, it's fairly certain not to be disinterred for many years.³¹

Handling and disposal of the corpse can be messy if the plan includes transportation to another location. As experienced police officers know, violent death is rarely neat or clean, and many targets vomit, or void their bladders and bowels as they die.³² A body bag is a useful accessory to avoid soiling a vehicle during transportation.

Logistics for the execution can be simple and straight-forward. Obtaining a firearm or other weapon is routine for police officers because they often confiscate weapons from suspects and withholding an occasional one from the property office can build up a small supply of weapons not traceable to individual officers. If a firearm has previously been used in a crime, ballistic evidence can lead an investigation away from the officers involved.

Handguns are in demand because of their concealability, although an occasional termination plan requires a knife, wire, or rope. Unlike what happens in spy films, poisons rarely figure in terminations because they take too long to act and aren't as reliable or easily available as firearms.

Obtaining a vehicle for transportation to and from the execution site, or to carry the corpse, is easy for big-city officers with access to "laundered" vehicles. Undercover and narcotics units regularly have their vehicles re-registered with legitimate but untraceable plates, and an

officer with a connection with such a unit can take advantage of the process.

Another way of terminating suspects is during a violent crime in progress. One police unit specialized in targeting repeat offenders. Unit officers would conduct surveillances while suspects were planning crimes and gathering weapons and other equipment. When the crime "came down," officers would act. The key was to interrupt the crime at the critical moment, making a gunfight inevitable. It was helpful if innocent lives were endangered by the suspects, because this would without doubt justify officers' use of deadly force.³³

Most police problems aren't as dramatic as the extremes of suspect handling. More common is justifying search and seizure.

Notes:

1. *Law Enforcement News*, NY, John Jay College of Criminal Justice, October 31, 1990, p. 2.
2. *L.A. Secret Police*, Mike Rothmiller and Ivan G. Goldman, NY, Pocket Books, 1992, p. 37.
3. *Ibid.*, p. 41.
4. *Police*, July, 1992, p. 56.
5. *Family Of Spies*, Pete Farley, NY, Bantam Books, 1988, p. 327.
6. *S.W.A.T.*, December, 1989, p. 68.
7. *Law Enforcement News*, October 31, 1990, p. 4.
8. *City Police*, Jonathan Rubinstein, NY, Ballantine Books, 1973, pp. 32-233.
9. *Ibid.*, p. 204.

52 Dirty Tricks Cops Use

10. *L.A. Secret Police*, p. 93.
11. *The FBI KGB War*, Robert J. Lamphere and Tom Shactman, NY, Berkley Books, 1987, pp. 208-209.
12. *L.A. Secret Police*, pp.180-181.
13. *Ibid.*, pp.181-183.
14. *Law Enforcement News*, October 31, 1990, p. 2.
15. *Law Enforcement News*, March 31, 1991, p. 2.
16. *Law Enforcement News*, June 15/30, 1991, p. 3.
17. *Law Enforcement News*, November 30, 1991, p. 2.
18. *Law Enforcement News*, November 30, 1991, p. 3.
19. *Law Enforcement News*, June 15/30, 1991, p. 3.
20. *City Police*, p. 190
21. *Ibid.*, pp. 183-184.
22. *L.A. Secret Police*, pp. 34-35.
23. *Ibid.*, p. 91.
24. *Ibid.*, pp. 137-138.
25. *Ibid.*, pp. 38-39.
26. *The Squad*, Michael Milan, NY, Berkley Books, 1992, pp. 54-107.
27. *Law Enforcement News*, March 15, 1991, p. 4
28. *The Squad*, pp. 3 & 6
29. *Ibid.*, p. 47.
30. *By Way of Deception*, Victor Ostrovsky and Claire Hoy, NY, St. Martin's Paperbacks, 1991, p. 206.
31. *The Squad*, pp. 64-66.
32. *Ibid.*, pp. 105-106.
33. *L.A. Secret Police*, p. 124

4

Search And Seizure

Searching suspects and seizing evidence have their own rules, established by statute and modified by case law and departmental policies. Officers must know the ins and outs of proper procedure to make a case stand up in court.

The need to secure evidence sometimes puts police officers in a dilemma. Basically, there must be "probable cause" or a search warrant to search premises, and failure of the officer to provide for one or the other results in the evidence's being suppressed in court. This is called the "fruit of the poisoned tree" doctrine. The purpose is to

54 Dirty Tricks Cops Use

persuade police officers not to use illegal search and seizure, because they won't be able to introduce any seized material as evidence in court. However, there are ways to obtain evidence without the taint of illegality

Dropping a Dime

This technique is to obtain probable cause to enter suspect premises. An investigating officer anonymously calls "911" to report that a "man with a gun" ran into the suspect premises. Another pretext is to report a fight or disturbance in progress. The police dispatcher sends a patrol unit, and when it arrives the investigators meet the uniformed officers. They announce that they just "happened" to be in the area, and offer to assist the patrol unit. Using this pretext, they enter the premises. Once inside, they can conduct a surreptitious search, plant evidence, etc

Break and Enter

Another way to obtain probable cause is to break the door or window of the suspect premises, and have a patrol unit respond. This is especially easy to work if the premises are protected by an alarm service. The alarm company will call the police, or an automatic dialer and telephone tape will call "911." As before, investigators in the area offer their services to responding officers.

Previously Planted Evidence

Exploiting certain knowledge that contraband is on the suspect premises is easier in some areas than in others. While many judges will grant a search warrant upon an affidavit that "reliable information" has disclosed that there is contraband upon the premises in question, a judge's cooperation depends upon consistent results. The majority of search warrants have to produce evidence to maintain the officer's credibility and that of his "confidential sources."

There are right and wrong ways to plant evidence. As we'll see during the discussion of entrapment, there are ways of using informers to plant evidence for later discovery by a search team. A basic way to plant evidence is what we call the "black bag job," surreptitious entry.

Surreptitious entry is a standard technique of intelligence and counter-espionage agencies. Stealing confidential material from foreign consulates is one way of discovering another government's secrets. American intelligence agents did this routinely during World War II.¹ The Federal Bureau of Investigation had a special squad of unofficial agents who served the same function during much of the cold war.²

"Black bag jobs" are not monopolized by security police. Regular law enforcement agencies break and enter to obtain information and evidence when nothing else works. Mike Rothmiller, a Los Angeles investigator, pored over a suspect's telephone records and noted that his target had made many calls to a particular

56 Dirty Tricks Cops Use

telephone in New York City. Obtaining the number's name and address from a cross-listing, he asked a contact of his in the New York City Police Department for information about that person.

When the New York detective contacted him shortly thereafter, he asked Rothmiller for a safe mailing address to which he could send some highly sensitive material. Rothmiller arranged with another police officer in another state to receive the package for him. The package duly arrived, containing address books, photographs, pieces of paper, and other material that had apparently been scooped up from someone's desk. The New York officers had broken into the target's premises and emptied out his desk drawers, sending the unfiltered material to Rothmiller for whatever he might make of it.¹ In this case, surreptitious entry served as a way to obtain evidence. It can also facilitate planting it.

Planting evidence can be simple or complicated, depending on the situation and the locale. One of the easiest ways is to drop a plastic envelope of marijuana through a partly open window onto a car seat. Many drivers, especially in hot climates, leave one or more windows open a crack to let hot air vent from the vehicle. A plainclothes agent can slip a "baggie" through the crack in a couple of seconds. The practical value of this technique is that many states have laws allowing police to seize any vehicle in which they find illegal drugs.

In some instances, other vehicles become the targets. Aircraft, much more expensive than cars,

often serve to smuggle illegal drugs over the United States' Mexican border. Narcotics officers also use them for aerial surveillance. More than one aircraft has come into the hands of narcotics agents because an agent "happened" to be walking around the airport and noticed contraband on a seat.

Planting evidence in locked premises is much more difficult. This is almost always a team operation. The team leader decides what is to be planted, and where. He directs a surveillance team to stake out the premises to discover when the occupants have left. A reconnaissance team tries to discover what locks and other security systems are in use. Once there's enough information to determine whether or not entry is workable, the team leader makes the final decision.

If he decides that it's practical to get in and out without detection, he chooses his team for the operation. The outer perimeter will require a surveillance team equipped with radios or cellular phones to warn if any of the occupants are returning. A security team may be necessary to delay the return of the occupants if circumstances permit. One delaying tactic is staging a traffic accident. Another, more drastic method is to stage an altercation with the occupants, with either a fake drunk or mugger accosting them.

The entry team consists of an officer trained in picking locks without leaving evidence of forced entry, such as scratches or tool marks. His job is only to open and relock the locks without leaving

58 Dirty Tricks Cops Use

traces. The 'bagman' carries in the contraband and places it in a suitable spot.

Some premises, such as 'rock houses,' are too tough to enter. Rock houses are fortified drug dealers' premises, equipped with fences, guard dogs, booby-traps, and other methods of detecting and impeding entry. These are usually occupied 24 hours a day, making surreptitious entry impossible. In such cases, police officers have to find softer targets, such as dealers' residences, if they don't live in the rock house itself, or their vehicles. Planting contraband in a vehicle is a double-barreled tactic, because it deprives the suspect of transportation, thereby cramping his style, as well as providing an asset for investi-gators.

An officer searching a suspect can "discover" evidence on his person, in his vehicle, or in his premises. Some agencies label this as "proactive policing." An officer can help make an arrest "stick" by falsifying his report, such as claiming to have witnessed a criminal act when he only heard about it from someone else. Prosecution is cleaner and simpler if the officer states unequivocally that he witnessed the act.⁴

There are subtleties to committing perjury to reinforce a case. One is not to mention any facts which may help the defense. "I can't recall" is a common ploy to avoid disclosing something which may weaken the case.⁵

Handling witnesses who may buttress a suspect's defense is delicate, and one way is simply to leave them out of the report. Police know that

overworked public defenders are unlikely to invest the time required to locate such witnesses.

When several officers are involved in an arrest, it's necessary to hold an informal conference to reconcile their statements, to assure that there exist no weaknesses or contradictions that may sabotage a case. It's often necessary to "doctor" arrest reports to simplify and strengthen the case, and officers must agree on the statements they'll provide in their reports and in court."

"RICO" Statutes

During the last two decades, several laws at federal and state levels have come into being to hit harder at organized criminals. These are generally known as "RICO" (Racketeer Influenced and Corrupt Organizations) laws, and provide for summary confiscation of assets from criminals. RICO laws have become valuable enforcement and prosecution tools.

If a police officer walking by "happens" to notice a "baggie" on the seat of a sports car belonging to a narcotics suspect, he can seize the vehicle. With a paint job and a new set of license plates, the car is ready for use by undercover investigators, without straining the agency's budget. This provides incentive for investigators to plant evidence enabling them to seize vehicles.

Another important aspect is that seizing assets can hamper a suspect's defense. Confiscating a bank account or other liquid assets thereby makes prosecution easier because without the funds to

60 **Dirty Tricks Cops Use**

pay a private attorney, the suspect has to rely on the public defender. Public defenders are typically inexperienced and overworked, with caseloads as heavy as those of police officers. A typical public defender is a recent law school graduate using the post to obtain experience before trying for a more lucrative job.

The typical public prosecutor comes from the same background as his counterparts in the public defender's office, and is no match for a tough and experienced trial lawyer. Affluent suspects who can afford to hire the best legal talent may never see the inside of state prison, stringing the case out with legal delaying tactics, until arresting officers and key witnesses have forgotten, moved away, or died. Even if convicted, they have a series of seemingly endless appeals to postpone serving the sentence. Depriving suspects of these options is a powerful weapon, which is why police officers and prosecutors alike welcomed the RICO laws.

Pitfalls in Serving Warrants

A search warrant affidavit is a legal document, and it's vital to get every detail right. Incredibly, some officers have compromised their cases and put themselves and their agencies in line for megabuck lawsuits by making simple errors, such as writing the wrong address on the affidavit. An innocent error can lead to charges of wrongdoing, even when the case is otherwise solid.

This has happened all over the country, with a variety of results. In Guadalupe, Arizona, police raided the wrong house because the case officer had not made a proper reconnaissance. In this instance, householders were very forgiving of the error. In another instance, federal drug agents broke the door of the wrong apartment, frightening the two young ladies inside. They apologized, repaired the door, and that ended the incident. However, in Kent, Washington, police served a search warrant at the wrong address in full view of a TV crew taping the popular program, *Cops*. TV crews captured footage of the husband and wife, and their four children, being dragged out of bed at gunpoint. The half-naked wife had her posterior recorded for posterity by the camera, although an officer later covered her. The problem arose because the wrong address was on the affidavit and warrant, and the case officers were not in the front line to show the raiding party the correct address next door.¹

Taking short-cuts in law enforcement is risky, but as we've seen, a careless and innocent error can have serious consequences. The householder whose front door has been demolished by eager officers will be frightened and angry, and it's only a short trip to Jacoby & Myers.

Notes:

1. *Surreptitious Entry*, Willis George, Boulder, CO, Paladin Press, 1990, pp. 102-111.
2. *The Squad*, Michael Milan, NY, Berkley Books, 1992, p. 3.

62 Dirty Tricks Cops Use

3. *L A Secret Police*, Mike Rothmiller and Ivan G. Goldman, NY, Pocket Books, 1992, pp. 163-164
4. *Ibid.*, pp. 31-32
5. *Ibid.*, p. 31.
6. *Ibid.*, pp. 32-34.
7. Associated Press, May 25, 1992.

5

Informers And Information

A police officer's stock in trade is information, obtained from a variety of sources. Long before modern scientific investigation, police obtained information from people, as they still do today. People may be victims, witnesses, or associated with the suspect. The suspect's associates may be relatives, friends, employers, and others who have any dealings with him. These may include hotel clerks, prostitutes, co-conspirators, and others.

Police officers increasingly obtain information from inanimate sources, such as city directories

64 Dirty Tricks Cops Use

and computers. We'll examine these carefully, because they're becoming increasingly important to investigators.

People

People who provide information to officers fall into two classes: *informants* and *informers*. Informants are those who have information that will enable police to find, apprehend, or convict the suspect, without being directly involved with his criminal activities.

Informants

Informants can be witnesses, passers-by, neighbors, and others. They may also be members or employees of private and public companies and departments. A contact in the Internal Revenue Service can disclose a lot about a suspect to investigators. One type of contact highly prized and used by police investigators is the former law officer working a security job with a private company. Many large corporations, such as credit reporting bureaus, hire former law officers as their security directors, and this network of former cops helps investigators obtain sensitive information without the formality of an official request or a court order.

Using such sources, investigators can obtain a suspect's telephone records, credit card records, bank records, and other privileged information. Former police officers who run their own private investigative agencies often have access to infor-

mation outside normal police channels, and they cooperate when former colleagues ask for help.¹

Informers

Informers are criminal associates, or people who inform for pay or other special consideration. Police and journalists often confuse these terms and use them interchangeably. Obtaining information from informants is fairly routine, requiring patience and good interviewing technique. Handling informers is another matter because informers always stand to gain from their relationship with the police, and indeed often initiate the contact in the hope of obtaining something for themselves. Informers often have criminal records themselves, and are not above fabricating information to sell for personal gain.

Informers' Motives

Informers operate from a variety of motives, all centering around personal gain, which need not be monetary. Drug dealers sometimes snitch on other dealers, using the police to suppress their competitors. An informer may "put the mouth" on a suspect for revenge. Yet another motive is to strike a "deal" with police or prosecutors, working for immunity or a reduced charge or leniency in their own problems with the law. Finally, there is payment, in money, drugs, or in simply being left alone to pursue criminal activities.

66 Dirty Tricks Cops Use

Officers sometimes allow prostitutes or professional gamblers to operate unmolested in return for a flow of information. Interrupting their business would result in breaking their contacts with the street, and information would dry up. It's expedient to allow relatively harmless offenders free rein to obtain information about heavy-duty suspects. This follows the principle of "trading up."

Handling Informers

Officers must always handle informers with a delicate touch, and keep them at arm's length. Informers have been known to "work both sides of the street." The snitch may be feeding false information to officers for money, or to falsely accuse someone else in return for their freedom. Another prospect is the double agent passing false information to officers to ingratiate himself with the suspect, or to save his life, because sometimes the penalty for snitching is death.

At 7 A.M. one summer morning in Phoenix, Arizona, federal agents raided an apartment occupied by a parolee who purportedly was dealing drugs. After the lead agent opened the door with his battering ram, agents rushed in to be nauseated by an overpowering odor of putrefaction. One agent thought that the apartment contained a corpse. Agents opened the windows, turned on the air conditioner, to air out the premises. During the search, they found chicken parts in the garbage can, but no drugs. Belatedly, they realized that the occupant had not been

home all weekend, and suspected that he had left the chicken parts in a hot apartment for their benefit, as a practical joke.²

A basic principle in handling informers is always to insist on "trading up," as we've seen. The informer must always give better than he gets, or it isn't a profitable deal for the officer or prosecutor. There's no percentage in letting a burglar go to arrest a jaywalker.

Informers are notoriously venal, and it's no exaggeration to say that some would even sell their mothers. They'll also sell out the control officer, which is why officers handling informers must always guard against lies, using the carrot and the stick. The "carrot" is payment for information, which works well with some trustworthy informers who value both money and the officer's esteem. This "positive reinforcement" is not enough with others.

For difficult cases it's always smart to keep the "stick" in reserve. Experienced officers know that having a "twist," or threat, to use against an informer who plays dirty is often the only way to keep him in line. A "twist" may be the threat of sending the informer back to prison, or threatening to leak the news that he's passing information to the cops, which can lead to a death sentence from his underworld buddies.³

Cross checking informers' statements is necessary because of their propensity to fabricate information to please the control officer and collect payment. If possible, the officer should have two informers, both unknown to each other, providing information on the same target. If the

information doesn't reconcile, the officer knows that something is wrong.

Cross-checking can become very elaborate, especially when another agency becomes involved. Agencies trade informers and information, but they don't always play fair with each other. One agency may hold back information, or pass on bad information, because rivalry and territoriality still exist in police work. This is especially true when federal agencies deal with local ones.

In one case, a police investigator learned that a former "mob" member had moved into his area. The local FBI office was using him as an informer because he'd already provided evidence in a case against the mob and was under the protection of the Federal Witness Protection Program. FBI agents reasoned that the former mobster had local mob contacts and would be able to provide information regarding their activities.

The police investigator interviewed the mobster, who told him that he wasn't telling the FBI much of value, because FBI agents were easy to fool. He told the officer that providing the FBI with good information would expose him to danger, now that he was trying to keep a low profile and begin a new life. The FBI was paying him \$1,500 per month for his bogus information. The police investigator compared the information he obtained from this informer with what the FBI said he had told them. The local investigator was suspicious that the FBI wasn't sharing all of the information they'd obtained. Later, the investigator told FBI agents that their informer wasn't spilling all he knew, but they didn't take him

seriously because of their boundless self-confidence.⁴

Crossing The Line

Informers sometimes cross the line into another category, the "agent provocateur." This is an instigator who leads his associates into committing an act for which they can be arrested and indicted. We'll study case histories of instigators in later chapters.

Using Computers

As we've seen, computers can be very useful in finding local fugitives. Tapping into utility company computers is common, but finding suspects who are long gone requires wider and more imaginative use of modern databases.

A "database" is a computerized collection of information, such as a suspect's name, address, drivers license number, social security number, numbers of his credit cards, etc. Using such databases enables tracing someone literally across the country.

Some of the databases that help trace people are: credit reporting company records, airline reservation computers, Social Security Administration files, Internal Revenue Service computers, welfare computers, and bank computers. Bank computers can be especially useful because they can provide almost hourly locations of people who use credit or debit cards habitually.

70 Dirty Tricks Cops Use

These databases are in common use by private investigators, who often gain access to data files in total secrecy.⁵ An example is tracing missing spouses in civil actions.⁶

Law enforcement agencies find computer tracing very useful, especially in today's climate of mobile and sophisticated lawbreakers. The FBI's NCIC, accessible by practically all law enforcement agencies in the country, has proved its worth in over two decades of operation. The Internal Revenue Service uses computerized matching to compare declared incomes against lifestyle databases to find those who are living beyond their officially declared incomes.⁷ This is easy to do, because comparing credit card purchases and automobile registrations against individuals' Form 1040s discloses those who claim modest incomes, yet own expensive cars and charge opulent vacations.

FinCEN (Financial Crimes Enforcement Network), for example, enables tracing money launderers trying to "lose" illegally-gotten assets.⁸ Gathering information about money movements and generating profiles of the individuals concerned enables building up an accurate picture of illicit financial transactions and the people who perpetrate them.

TECS II (Treasury Enforcement Communications System, Version II) is a computerized 'watch list,' a database of undesirables useful to customs agents and other police forces at ports of entry. This allows checking everyone who tries to enter the United States against a master list of possible suspects. Port of entry checking goes

beyond identifying criminals. This is also useful for government security agents trying to identify foreign agents trying to enter the United States.

The United States is not the only country with computerized watch lists at ports of entry, as this is common practice throughout the world as a basic frontier security measure. Early detection of foreign agents and their couriers allows tracing them within the country from the first moment, and this can lead to uncovering their contacts and associates.

Persistent investigators need not worry about various restrictions placed on the dissemination of privileged information. As we've seen, the network of former police officers cooperates in extracting privileged information from restricted databases.

Fortunately for law enforcement, various "privacy acts" exempt law enforcement agencies from limitations placed upon privately-operated information-gathering services. However, this may change, perhaps because of abuses and breakdown of security. The General Accounting Office found that TECS II has its problems. There was a high percentage of errors, which could lead to effort wasted in investigating innocent people, and one suspended employee of TECS II was illicitly gaining access to the database.⁹ This leads to the need for greater security.

Information Security

A basic principle in operating any law enforcement intelligence operation or network is

72 Dirty Tricks Cops Use

secrecy. One reason is to prevent the bad guys from knowing how law enforcement officers may track them, and therefore devising counter-measures. Another reason has to do with public reaction. Large-scale information gathering necessarily spreads an electronic dragnet that includes a majority of people innocent of any crime, just as a drunk driver roadblock inconveniences and delays many perfectly sober motorists. This creates a ready-made issue for civil libertarians, a necessary evil in a free society.

The public remains necessarily unaware of thousands of well-conducted and successfully concluded investigations aided by computer tracking of suspects. However, one abuse or mistake can lead to serious consequences as injured innocent parties are manipulated by self-seeking lawyers and politicians. Attorneys, of course, enjoy a major lawsuit against the government, because they're almost guaranteed excellent remuneration for their efforts. Politicians, especially those with minority constituencies, have a ready-made campaign issue when they can posture against "racism." That a computer cannot be bigoted is irrelevant to politicians, who find championing minority causes a ticket to certain re-election.

This is why all law enforcement activities involving computer databases must remain top-secret. It's important to assign only the most trustworthy officers to such duties, officers who have proven themselves and their integrity in other sensitive assignments. Some agencies with

secret investigative units impose a Mafia-like secrecy on their activities.¹⁰

There are many methods of maintaining and enforcing secrecy of paper and electronic intelligence files. A basic way is to keep them off police premises. Officers' homes, and privately rented storage facilities serve the purpose, ensuring that no unauthorized police personnel will accidentally discover them. In one case, detectives transferred a triplicate file to a public storage locker, which a detective had rented in his own name and paid for with cash taken from a slush fund.¹¹

Another reason for private storage of files is to put them beyond the reach of organizations such as the American Civil Liberties Union and court orders. It's impossible to subpoena material if you don't know it exists, or where it may be.¹² Today, sensitive files take up little space when stored on high-density computer disks. The ease of duplicating disks ensures that vital files need never be lost, even if a politically-minded chief decides to disband the unit.

It's also important not to allow any information about these projects to become public knowledge, under any circumstances. An enterprising journalist, given a glimpse into the massive amounts of data on individuals available to law enforcement agencies, can generate an immense amount of publicity that can kick back against the agencies concerned.¹³

Gathering information is an important step towards clearing the case. After arrest comes a process that can save valuable time if it works. This is obtaining the suspect's confession.

Notes:

1. *L.A. Secret Police*, Mike Rothmiller and Ivan G. Goldman, NY, Pocket Books, 1992, pp. 165-166.
2. The author witnessed this incident.
3. *L.A. Secret Police*, p. 93.
4. *Ibid.*, pp. 135-136.
5. *Privacy For Sale*, Jeffrey Rothfeder, NY, Simon & Schuster, 1992, pp. 63-88.
6. *Ibid.*, pp. 106-112.
7. *Ibid.*, p. 142
8. *Ibid.*, pp. 136-137.
9. *Ibid.*, pp. 138-139.
10. *L.A. Secret Police*, p. 21.
11. *Ibid.*, p. 9.
12. *Ibid.*, p. 19.
13. *Ibid.*, p. 23.

6 Obtaining Confessions

Once a suspect is in custody, police and prosecutors combine efforts to obtain confessions, for several reasons. The evidence leading to the arrest may be weak, and a confession wraps up the case and makes conviction almost a sure thing. Another reason is that a confession makes a lengthy trial unnecessary, thereby saving on police, prosecutorial, and court costs. With suspects too poor to pay their own lawyers, the state saves on the cost of a court-appointed lawyer. Confession is often a prelude to a plea-bargain.

76 **Dirty Tricks Cops Use**

Some suspects decide to tough it out because they're ignorant of the nature of the evidence. Once a defense attorney gets into the picture, he may advise the suspect to plead guilty to a lesser charge, or in return for a lighter sentence.

The basic rule here is that the earlier a defendant confesses or pleads guilty, the better deal he's likely to receive. If he decides to fink on his companions before police file charges with the prosecutor's office, he may avoid prosecution altogether. In some cases, the suspect may be able to obtain immunity by "trading up," which means providing information on someone suspected of a more serious crime, even if the object of his disclosures is unconnected with the present charge.

Emotions, Confession, and Irrational Decisions

Emotions can play a major role in obtaining confessions. Suspects often act against their best interests because of the effect of overpowering emotion. Guilt, for example, plays a major role with situational offenders such as the hit and run driver. A minister arrested for molesting children will almost certainly feel acute embarrassment and guilt, and the investigating officer can use these feelings to elicit a confession.

At times, simply telling a suspect that he'll "feel better" if he gets it off his chest will persuade him to confess. The officer carefully leads the discussion away from how the suspect will feel while he's spending several years in prison. The officer's appeal is to emotion, not logic. This is the

principle behind sympathy ploys and other emotional tricks.

Sympathy ploys don't work well with the habitual offender and street-smart suspect. He's not vulnerable to appeals that he'll "feel better if he gets it off his chest" and other nonsense. With this type of suspect, it's better to appeal directly to his self-interest, using "deals," falsified evidence, and intimidation.

Investigators are also vulnerable to emotion, and sometimes make irrational decisions. This is most likely in high-profile cases in which they receive a lot of "pressure" to make a case. The investigator swayed by emotion instead of logic can go into an interrogation convinced that the suspect is guilty, and obtain a confession, despite the lack of corroborating evidence.

With enough intensive effort during interrogation, many innocent people will confess. Officers tempted to speed the process by coaching their subject unwittingly pass investigative keys to him, then listen to the subject feed them back during his confession.

One noted instance was the Wylie-Hofert murder in New York City, during the early 1960s. Two young ladies in their early 20s were sodomized and killed, and because one victim was the niece of Phillip Wylie, the novelist, pressure on the police was intense. Her father, Max Wylie, although not as famous as his brother, had important connections. Police arrested a young man and interrogated him, and his confession contained important investigative keys, such as the role of a jar of Noxema in the

78 Dirty Tricks Cops Use

rapes. It later developed that the confessed suspect had an unbreakable alibi, and police had to release him.

More recently, nine people were murdered at Wat Promkunaram, a Buddhist temple just west of Phoenix, Arizona, in August, 1991. This mass murder immediately developed international complications, with the Thai Government concerned with its solution. Maricopa County Sheriff's investigators received a phone call from an inmate of a Tucson psychiatric hospital, stating that he and several others had committed the murders. Sheriff's officers, desperate for a break in the case, took the psychiatric patients' statements at face value, and arrested him and three others. They confessed after intensive interrogation, and sheriff's officers conducted a fruitless search along the freeway between Phoenix and Tucson looking for evidence allegedly discarded as the suspects drove back to Tucson. The suspects later retracted their confessions, stating that they had been coerced.

In November, 1991, Air Police at Luke Air Force Base stopped a youth and discovered a firearm which turned out to have been the murder weapon in his vehicle. This development, supported by physical evidence, forced a re-evaluation of the case against the first suspects. Eventually, two young men living in the Phoenix area were charged with the crimes. Sheriff's officers had to release the original suspects. Three of the original suspects have filed suit against the Maricopa County Sheriff's Office.¹

Miranda

The "Miranda" Decision, delivered by the U.S. Supreme Court almost three decades ago, established that police officers must advise suspects of their rights when they take them into custody. The key word is "custody." No Miranda Warning is necessary during the early stages of an investigation. This greatly helps the investigator because suspects may still think that by appearing cooperative, they'll deflect suspicion from themselves. A suspect confident that he can "talk his way out of it" leaves himself vulnerable to low-key interrogation until the moment the officer has enough evidence to make the arrest. Of course, the private detective or security officer does not have to give a Miranda Warning, because the Bill of Rights was designed to protect citizens only from the government, not from other citizens.

Today, police agencies issue officers Miranda Cards, giving the form of the warning. Some agencies issue bilingual cards, with "Miranda" in both English and Spanish. Others have a space for the suspect to sign at the bottom, to acknowledge that he did receive the Miranda Warning. Although tradition-minded officers curse the Miranda Decision, saying that it makes their work harder, there are many ways to obtain confessions from suspects, and police still manage to keep the jails full.

Circumventing Miranda

American police officers have developed several ways to lessen the effect of Miranda upon

interrogations. While they still read the suspect his rights, to conform to the judicial requirement, they sometimes deliver the warning in an off-hand manner, implying that it's only a formality.² Another way is to avoid giving the warning, but stating that they did if the matter comes up in court. This is perjury, but in many cases judges and juries will believe the officer over the suspect.³

Immediate Confession

Suspects are often emotionally most vulnerable upon arrest. This is why it's important to make a maximum effort to isolate and disorient them once the handcuffs are on. A store security officer (private security officers are not obligated to "Mirandize" suspects) will bring the suspect to a back office, away from familiar places and faces. Police station interrogation rooms are always hidden away, preferably without windows, to remove the suspect from anything familiar and comforting.

It's at this emotionally most vulnerable moment that police and security officers can press for an immediate confession, sometimes by exaggerating the charges. Telling the suspect that he's the one responsible for a string of robberies or auto thefts can bring the admission that he only carried out one or two.

Interrogation Ploys

There are many tricks and techniques of interrogation, developed by hard-working police

officers over many years of experience. Most fall into one of several classifications. There are "hard-line" approaches, and several varieties of softer methods. Officers use deception with a clear conscience, knowing that most suspects lie to them, anyway. Pretending sympathy, blaming the victim, and other emotionally dishonest tactics are normal in manipulating suspects into confessions. Sympathy is likely to work with the situational or first-time offender, such as an employee who stole company property, but with street-wise career criminals, it's necessary to take a stronger line. Emotional or physical brutality are the only languages they understand.

"Let's Make a Deal"

Any street-smart suspect knows his rights, whether the officer advises him or not. Suspects watch TV cop shows too. Theoretically, hardened career criminals should not say a word to the arresting officer, and demand to see an attorney immediately. In real life, it's not that simple. In fact, some suspects are eager to make a deal.

Police and suspects alike know that there rarely is honor among thieves, and that one will sell out another to secure an advantage for himself. In some cases, there's a race between arrested suspects to cut a deal that will result in a lighter sentence, even if it means testifying against a partner in crime. Some will even place all of the blame upon their partners in an effort to convince officers that they played only minor roles in the crimes. There are several techniques

82 Dirty Tricks Cops Use

officers can use to improve their chances of persuading a suspect to make a deal.

Divide and Conquer

Playing one suspect against another is a favorite technique that takes advantage of criminals' distrust of each other. It's necessary to keep arrested suspects separate, so that they cannot compare notes. This allows the interrogator to mislead the suspects and manipulate their minds.

"Your Buddy Confessed"

Telling one suspect that his partner has confessed is a trick to use against a suspect who's not too bright. Truly street-smart suspects understand that confession is a race between contenders, and that after one has confessed and made the prosecution's case, officials don't need confessions from the others. This is a stupid way of playing one off against the other, but it still works at times. The only benefit for police and prosecutors is to simplify prosecution and save on court time.

A variation on this trick is to separate a pair of suspects, then bring one to the interrogation room for a period of time. It's not necessary to actually speak with the suspect, just to give his partner the impression that he's being interrogated. When the officer brings the suspect back to his cell, he thanks him for his cooperation within earshot of the other and promises to try to "do something" for him. He then takes the other

suspect in for interrogation, letting him worry about what his partner confessed to the officers.⁴

A variation on this technique is to leave one of the suspects in an outer office while questioning his partner. After awhile, the officer calls out to his secretary to come in to take a statement. After a period of time, the officer leads the partner back to his cell and brings the other suspect in for questioning. The time spent wondering what his partner said softens up the suspect, making him amenable to a deal.⁵

Graymail

Not all suspects seeking to deal roll over and play dead. At times, their position allows them to be very aggressive and demanding, and deal negotiation then becomes a two-way street because police and prosecutors don't hold all the cards. This happens when the suspect uses "graymail."

"Graymail" is the art of threatening to reveal very damaging information at the trial if the prosecutor insists on pursuing the case. At times, corruption reaches so high in a police agency or its parent government body that there's intense pressure to abandon prosecution and let sleeping dogs lie. An example is the house of prostitution patronized by judges and politicians, which enjoys relative immunity. When "the fix is in," police must tread carefully.

Another example comes when the suspect's activities can open a can of worms if revealed. One case that came to light was the prosecution of a person identified only as "Jim" who was

84 Dirty Tricks Cops Use

arrested for attempting to bribe an Internal Revenue Service clerk for taxpayer information. "Jim" was an underground trafficker in computerized information, culling it from credit bureaus, and a variety of legal and illegal sources.

The background to this case is that there is an underground industry furnishing supposedly private information about individuals to private investigators, credit bureaus, and other parties who pay the fees. Some of this information comes through strictly illegal means, such as purloining telephone company records for unlisted numbers, and private investigators posing as medical personnel to raid hospital records. Bribing government employees to hand over restricted documents is another illicit method, but it's very successful and widespread because it's strictly *sub rosa*.

The clerk accepted Jim's offer and immediately reported the incident to superiors. The IRS investigated, and soon Jim was under indictment for trying to blackmail a federal employee and for dealing in illegal information. However, Jim had a ready countermove, because during his career he'd amassed information about the rich and famous, such as Sylvester Stallone, General Richard Secord, boxer Michael Spinks, and other notables. He threatened to bring this information out in court, causing scandals, and this brought the prosecutor to heel.

The result was that Jim obtained a sweetheart deal, instead of a long and harsh prison sentence. He was not to do anything illegal for a year, and for six months operated as an informer for the

IRS and FBI, helping them with investigations of other information-gathering agencies involved in culling data from restricted government files. The icing on the cake was that Jim was actively helping federal law officers to shut down his competitors, as well as being able to pursue his own business almost unmolested.⁶

Sympathy

Pretending to sympathize with the suspect to make him or her open up is worthwhile, especially when the suspect is not a street-smart and hardened criminal. The purpose of sympathy ploys is to relax the suspect by making his crime appear less significant than it is, so that he feels more comfortable discussing it with the interrogator. This can be very effective with a person accused of assault during a domestic dispute, for example. The interrogator who sympathizes with the suspect, admitting that he's been tempted at times to use force on his wife, improves his chances of eliciting a voluntary confession.

"Everyone Does It"

The investigator attempts to dilute the emotional charge of guilt and shame by sharing the guilt. An example might be shoplifting or employee theft. The police officer takes advantage of the common knowledge that many people steal small items, especially from employers.⁷

The "everyone does it" technique leads into another ploy, "salami-slicing." This is cajoling a confession from the suspect in installments

86 Dirty Tricks Cops Use

instead of one dramatic breakthrough. The officer begins by suggesting that the suspect surely must have thought of taking something at one time or another. With this critical first admission, the next step is to suggest that he may have stolen something insignificant, then something of more value. Step by step, the suspect admits to greater and greater misappropriations until he confesses the crime in question.

Blame the Victim

This is a crude attempt to mitigate or erase the suspect's guilt by shifting the blame onto the victim. Again, in a case of employee theft, the officer states that the employer is cheap and exploits his hired help, thereby justifying the theft. In cases of date rape, the officer takes advantage of the common knowledge that some women practice sexual teasing, and he gives the suspect absolution for having raped his date.⁶

Blame Society

This variation on the theme of absolving the suspect from guilt is effective because it takes advantage of the fashionable belief that "society" is somehow at fault for individual transgressions. Some suspects have a self-pitying attitude that sets them up for this ploy, and the interrogator can use this as an opening to elicit a confession. Feigning sympathy for the suspect by recognizing that he's had a hard life resulting from a broken home, ghetto upbringing, etc., can give the impression that the interrogator is on his side, after all.

Flattery

Another way of playing on a suspect's emotions is by flattering him on the skill he showed in his crime. Praising his skill as a fraud artist, safecracker, or burglar can pump up his ego so that he's more willing to describe exactly how he did it.⁹

Psychological Plays

At times, investigators have a suspect, but no evidence. In other cases, they have solid information, but from an informer they wish to keep in his undercover role. This rules out having the informer testify in court. Then it becomes necessary to use psychological trickery to obtain evidence and a confession. Publicized instances of these methods include FBI agents' interrogations of espionage suspects.

Ronald Pelton was a National Security Agency employee who allegedly had sold cryptographic information to the Soviets. The FBI had only the word of a defector who had since redefected to the Soviet Union, and a tape of a wiretap on the Soviet Embassy, made in 1980. On this tape, Pelton spoke in very guarded language about "something I would like to discuss with you. I think that would be very interesting to you." This was worthless as evidence, because it was so vague. However, FBI agents reasoned that it might work as a psychological lever to pry Pelton's lips open.

In November, 1985, FBI agents rented rooms in the Annapolis Hilton to provide a neutral

setting, and one agent telephoned Pelton, asking him to come to the hotel to discuss a matter of "extreme urgency." Three agents took chairs in an arc around Pelton's chair, so that Pelton would have to turn his head to speak to one or another. One agent told Pelton that he was going to tell him a story, and asked him to keep silent until he'd finished. The agent then began a tale about a young man from Pelton's home town, and told how he had followed a career in the Air Force and the NSA, and finally phoned the Soviet Embassy to offer to sell classified information. The agent obviously tailored the story to resemble what he thought Pelton had done. He then played the wiretap tapes, then asked Pelton to finish the story.

Pelton wasn't biting yet, and he replied that the story, while interesting, did not describe him. When the agent replied that it was Pelton's voice on the tape, Pelton countered by stating correctly that the tape did not make a case.

The agents continued the mind game, teasing Pelton with vague hints about "cooperation," trying to imply without actually committing themselves that they wanted him as a double agent. When Pelton stated that he'd want to consult an attorney before committing himself to helping the FBI, the agents replied that having an attorney present would only complicate the situation because security needs would mandate that the attorney would have to be cleared first. This was on the thin edge of legality, because if Pelton had stated clearly that he wanted to speak with an attorney right then, the agents would

have been obligated to discontinue the interrogation.

Now was the time for equivocation and a little deception, using ambiguous language that hinted, but did not state, that Pelton would not be prosecuted if he cooperated. An agent pointed out that "...many cases involving national security just do not result in prosecution."

Pelton fell into the agents' trap, believing that they had more evidence against him, and convincing himself that the government would not prosecute if he opened up and revealed everything. After answering many more questions, the agents kept up the charade by telling him that he was free to go meet his girlfriend. Actually, agents kept a close tail on him and at 9:30 that evening, an agent telephoned Pelton to tell him that they urgently needed to meet with him at the hotel. Pelton, having had a few drinks and a narcotic bought on the black market by his girlfriend, was relaxed and his guard was down. Agents counted on fatigue dulling Pelton's mental processes enough so that they could prod him into revealing incriminating information.

Under questioning, Pelton revealed where and when he'd met his Soviet contacts, and provided more details. Then came the question that agents felt was vital to making a case that would stand up in court. An agent asked him if he had been aware that turning over such information to the Soviets would harm the United States. Pelton, after some equivocation, admitted that he knew that passing the classified information to the

90 Dirty Tricks Cops Use

Soviets would harm American interests. Soon after, an agent "Mirandized" and arrested him.¹⁶

FBI agents used a similar mixture of hints and bluffs to cajole another espionage suspect into confessing. This was Larry Wu-Tai Chin, a Chinese-born former employee of a CIA subsidiary. Chin had begun working for the United States in 1948 as a translator for the U.S. Army Liaison Office in Foochow, China. He moved up to the U.S. Consulate in Shanghai, and ended up with the CIA's Foreign Broadcast Information Service. This service keeps watch on foreign media.

Although Chin was not cleared for classified information and his nominal job description did not give him access to classified information, he worked hard and earned the confidence of his superiors. Informally, he gained access to secret material because CIA personnel often needed documents translated, and they cut red tape to do it. Chin obtained American citizenship and a security clearance, and continued to pass secrets to the Red Chinese until he retired from the CIA in 1981.

FBI agents used a similar psychological approach to conceal their cards, because they'd obtained information from a double agent they wished to protect. An agent told Chin stories about two hypothetical people, one of whom cooperated with the FBI, and the other who did not.

Chin hoped to avoid prosecution and bit down on the hook, suggesting that he'd be interested in becoming a double agent. FBI agents told him that he'd first have to divulge

everything he knew. Holding out the hope of immunity, they milked him dry, then arrested him. His trial resulted in conviction, based mainly on material he'd provided.¹¹

Psychological ploys can be very effective against suspects who are not street-smart, and who are vulnerable to bluff. Bringing a white-collar suspect into a room with surveillance photographs of himself adorning the walls can convince him that officers have been watching his every move, and already know everything. This is intimidating, and provides the setting for a variant of the tricks used on Pelton and Chin.

"We already know all about what you did. What we need is information about your conspirators. Help us with that and we can make a deal." This offer, with the implication of immunity, can pry open the lips of the guilty but naive suspect.

Deception

At times, sticking strictly to the facts doesn't have enough effect, and it's time to try something stronger. With criminal suspects, it's morally correct to deceive, by implication, mis-statement, or omission, to obtain cooperation. It's also correct to appeal to the suspect's need for a favorable outcome, turning this into self-delusion. This is the basis of the first technique:

Dropping The Charges

Persuading a suspect that charges against him will be dropped if he confesses may appear

92 Dirty Tricks Cops Use

incredible to the reader, but to a suspect under severe emotional tension it can be made realistic. This depends upon two points: that the crime not be too serious, and that it's up to another person, rather than the law, to press the case. For example, a suspect accused of theft might be willing to believe an interrogator who tells him that, if he confesses, he'll have his employer drop the charges. Once the detective has the confession, he sends the suspect back to his cell. He can always explain later that the employer did not agree to drop the charges. Even if the suspect later realizes the deceit, and that the officer reneged, what can he do?

This can also work when the investigator needs information about another case or suspect, and can persuade the suspect that the prosecutor will consider dropping the charges in return for cooperation. It won't work if the investigator has to put it in writing, which will almost inevitably be so if the suspect has his attorney with him.

A variation on this theme is the "Can you take it back?" ploy. The officer implies that if the thief returns the stolen property the victim will drop the charges. The officer must be careful not to make a direct commitment, or put anything in writing.¹² Obviously, this sort of arrangement won't pass if the suspect's attorney is present.

The Fake File

Using a fake or phantom file can serve to undermine any of the suspect's statements that an officer cannot challenge directly. This trick requires a prop, a file folder, with a few sheets of

paper inside. When the suspect makes a statement the officer considers questionable, he can simply open the file, pretend to read for a few seconds, and reply, "That's not what it says here."¹³

Overcoming objections and challenges from the suspect is just as easy, because the officer simply uses the authoritarian approach. If the suspect asks what it says in the file, the officer can simply reply, "You're not asking the questions here. I am!"

The Phantom Charge

One way of prying a confession to a certain crime from a suspect is to convince him that he's under suspicion for something far worse. A suspected burglar can be told that he's under suspicion for a murder committed on the street next to the site of the burglary. A variant is to ask the burglar to explain the corpse found on the premises after he left, making it appear as if he'd murdered someone during the crime. Yet another variation is to exaggerate the amount of a theft or robbery. In all these cases, the suspect may take the opportunity to "trade down," confess to a lesser crime to avoid being charged with a more serious one.¹⁴

Minimizing The Charges

This is almost the reverse of the phantom charge, and some suspects lead themselves right into this set-up. A suspect eager to deal may not only sell out his partner, but try to inflate his partner's importance and minimize his own role

in the crime. Pretending to accept the suspect's statement as absolutely correct in every detail helps make the breakthrough to obtain the confession. Even with its distortions, the confession works as a lever in breaking the rest of the case. Faced with a partner's confession, especially if it's exaggerated and places most of the blame on him, a suspect may retaliate and confess the crime as it really happened. The prosecutor can resolve any discrepancies during the trial, and indeed use the contradictions to impeach the suspects' credibility.

The Accident

Another way of minimizing the charges is to suggest that the deed was the result of an accident or mistake of some sort. This works especially well if the suspect has already begun to rationalize his role in his own mind. Some suspects, desperate for a way out, grasp at any straw to deny or minimize their guilt, leaving the way open for the officer who knows how to exploit the opportunity. The suspect may be ready for the rationalization that he didn't really mean to steal something, but merely slipped it into his pocket and was later reluctant to disclose it because he feared being accused. In more serious cases, the officer may agree that the gun went off accidentally during a robbery that left the victim dead, for example. This is not the time to bring up the "felony murder" law, which states that any death during the commission of a felony leaves the perpetrator charged with first-degree murder, whatever the circumstances.¹⁵

"Let's Finish This and Go Home"

This is another outright deception that takes advantage of a suspect's yearning to put an end to his ordeal and be released from custody. It works best at the end of the workday or late at night, when the suspect is tired and not as mentally sharp as he was earlier. The interrogator tells the suspect: 'Look, let's get this over with. I know you're tired. I'm tired too. Let's wrap it up so we can all go home.' A suggestible suspect may accept the simplistic and naive proposition that confessing will bring him his freedom.

Intimidation

When softer approaches don't work, officers may try intimidation. There are many ways of intimidating suspects without using physical force. Sometimes, the mere suggestion of physical force can create anxiety in a suspect, which the cop can exploit. One or more husky, mean-looking cops can put fear into a suspect, without making any explicit threats.

The Mind Game

One way of intimidating the suspect is setting the scene for a mind game. Those who are not professional criminals, but white-collar criminals or occasional offenders are not sophisticated, and are vulnerable to this sort of intimidation. As previously discussed, candid photos of the suspect in various settings mounted on the wall,

for example, suggest round-the-clock surveillance.

"Innocent People Have Nothing to Hide"

This is a powerful technique that will work with all but the most case-hardened, street-wise suspects. Telling the suspect who wants to remain silent that innocent people have nothing to hide deprives him of the refuge of silence by making it clear that his very silence is an indicator of guilt. Logically, this suggests that the person is guilty until proven innocent, but the interrogator relies upon emotion, not logic, to win his case.

The interrogator can use this after delivering the Miranda Warning. Telling the suspect that he has the right to remain silent, but if he does, it's an indicator of guilt, can pry his lips open.¹⁶

The Suspect's Family

Intimidating a suspect by using subtle threats against his family can pry a confession from him, but only if it's clear that police actions will remain strictly within the law. Otherwise, working his family against him can backfire and break careers.

One way to do this is to emphasize how difficult it will be for the suspect's wife to cope with interrogation, if she's also a suspect. If not, pointing out how hard the trial will be on his family can be persuasive. Only by confessing himself can the suspect save his wife and family this ordeal. Another approach is to point out the hardships that his family will suffer as a result of

his imprisonment. Suggesting that his children will be subject to torment by classmates as a result of publicity puts the loyal family man on the horns of a dilemma. The alternative is to confess, make a deal, and receive probation instead of prison.

With a suspect who is not too bright, or fairly suggestible, it's possible to stretch this technique to outrageous lengths. The officer can tell him, "If you work with us now, your wife need not ever know about this." Alternatively, he can promise that the suspect's mother, neighbors, or other associates won't find out about his difficulties if he cooperates now. This defies logic, but it works with a few suspects.

Good Cop/Bad Cop

Another form of intimidation is to use the good cop/bad cop technique, also known as the "Mutt and Jeff" technique. This is the whipsaw approach, using both sympathy and threats, with one interrogator snarling and acting in a menacing manner, while his partner is sympathetic and conciliatory. The alternating "hot and cold" treatment breaks down a suspect's emotional resolve, and the surprising aspect is that this works, even on persons who know the trick, because it hits at gut level, not upper cortex. Detectives investigating the killing of a female motorist by a California Highway Patrolman used the good guy/bad guy technique against their suspect, Patrolman Craig Peyer.¹⁷

Tape Recordings

Some police investigators routinely tape record interrogations, both to ensure having an accurate record, and to be able to confront the suspect with his own words later. Tape recordings are valuable for intimidation, and they stand up in court.

Experienced investigators know that people who have just faced life-threatening incidents are emotionally aroused, sometimes not quite in control of themselves, and they may make statements that can later work against them. Recording a statement while a suspect is emotionally distraught can be very valuable, especially if incriminating.

Investigators don't always record statements, however. An example is a police officer who just shot and killed a robbery suspect. He may say something like; "When I saw that nigger pull his gun, I shot him." Investigators know that, if they record such a statement, or write it down verbatim, this can serve as justification for a wrongful death lawsuit, a peg upon which a civil rights group can hang a propaganda campaign, etc. Therefore, they do not tape record an officer's initial statement, only a sanitized version, and they go over his statement carefully with him before making their report. They do not extend such courtesy to civilians involved in shootings, even though the circumstances may be very similar.

Taping a Miranda Warning helps establish that the officers actually warned the suspect according to law. However, there are ways to fake

it. Leaving blank tape at the beginning of an interrogation allows inserting the Miranda Warning later. Clumsy officers, or those unsure of themselves, sometimes repeat Miranda Warnings to their detriment. Repeating it several times can alert even the stupidest suspects and induce them to shut up for their own good. Therefore, it's sometimes desirable to omit the warning, or delay it, until the suspect has made enough damaging admissions.

The "Plant"

A common way of obtaining information is using a "plant" in a prison cell. A cellmate can be an undercover officer, or a police informer. Even a genuine felon awaiting trial or serving time after conviction may be seeking material to trade for a "deal." One such was William Plew, whose testimony regarding a prison confession was important in the prosecution's case against Ruben Melendez, accused of stabbing another inmate to death in 1987. The complication came because Melendez sought help from a "jailhouse lawyer," allowed under Arizona Department of Correction rules. He chose Plew, who assisted him and later obtained parole for himself. Later, after his arrest for passing bad checks, he offered to "make a deal." Authorities had him slated as a key witness in Melendez' trial, but the issue of confidentiality obstructed the prosecution. The defense stated that, as Plew was acting as Melendez' attorney, the lawyer-client confidentiality principle applied, and Plew would not be allowed to testify.

Further complicating the issue was Plew's not being a licensed attorney, merely a jailhouse lawyer.¹⁸

This case illustrates the basic principle on covert information-gathering. An informer may provide valuable information to police and prosecutors, but even if the information is conclusive, bringing it into court is another matter. The dubious status of informers can make practical use of their testimony difficult or impossible.

Recently a case went up to the U.S. Supreme Court and established that an informer cellmate can provide testimony at a trial, circumventing the need for a Miranda Warning. This was *Arizona v. Fulminante*, Supreme Court No. 89-839. This cellmate, however, was not a jailhouse lawyer.

The conviction against Oreste C. Fulminante had previously been reversed in the Arizona Supreme Court, Case No. CR-86-0053-AP, on the grounds that "admission of defendant's involuntary confession was a reversible error," because the government informer had used implied threats to coerce the confession. The suspect had been convicted of killing his eleven-year-old stepdaughter, Jeneane Michelle Hunt, by shooting her twice in the head with a large caliber weapon at close range. At the time, police did not file charges, as the evidence was insufficient and contradictory, and Fulminante left the state.

Later, while Fulminante was serving time in a federal prison for an unrelated charge, he made damaging admissions to another inmate. Upon his release, the same inmate and his fiancée

picked up Fulminante at a bus terminal, and Fulminante stated that he could not return to Arizona because he had killed a little girl there. Police arrested him and returned him to Arizona for trial.

His appeal was based on the informer's telling him that he was in danger of physical harm from other inmates. Many inmates do not like "baby killers" and at times will assassinate them in prison. The informer told Fulminante that if he confessed to him, he would protect him from other inmates. The Supreme Court held that the confession was admissible, especially because Fulminante had confirmed it to the informer's fiancée upon his release, in circumstances which certainly were not threatening. The bottom line was that a "harmless error" did not call for automatic reversal of a conviction in this and other cases, a result of the *Chapman v. California* (1967) case.

Polygraph Examination

The polygraph, or "lie detector," isn't as reliable as its proponents claim, a fact which is becoming widely recognized in the law enforcement community. The polygraph measures only some physical symptoms of stress, none of which correlate reliably with truthfulness or mendacity. One of the original developers of the polygraph, John Larson, conducted a controlled experiment with the polygraph to test its reliability. He found it to be hopelessly inaccurate, and denounced polygraph testing as a "racket."⁹ Further

evaluation by the Office of Technology Assessment of the United States Congress found serious faults with it.²⁰ This is why criminal courts have disallowed use of polygraph "evidence" during the 70-plus years since the device appeared.

Even when investigators use the polygraph only as an investigative aid to determine a person's truthfulness, results can be contradictory. One aspect of its use in the recent Mesa, Arizona, Police Department sex scandal investigation shows this clearly. A major controversy was whether or not Mesa's Assistant Chief, Del Ballentyne, acted properly in pursuing the investigation after being told of widespread officer misconduct by an officer's wife. Cherie Staton, the wife of Officer Russ Staton, who was discharged and later convicted of child molestation, claimed that she had told Chief Ballentyne about other officers' sex escapades in 1988. Ballentyne countered with the statement that he did not recall Staton's making any such allegations to him. Cherie Staton took a polygraph test in 1992, and passed. Ballentyne at first refused, but then submitted to the test, and the polygraph showed him truthful, as well. This turned out to be a classic case of "What did he know and when did he know it?" but the polygraph proved to be no help at all in clearing up the question.²¹

From this, it's clear that the polygraph is as unreliable today as it was during its early developmental years. Nevertheless, the polygraph is still a valuable investigative tool. This is because the crafty investigator uses it as an

intimidation tool, taking advantage of suspects' credulousness and suggestibility. The polygraph technician makes every effort to convince the suspect that "the instrument will not be beaten," and thereby persuade him to admit the truth.²²

Some polygraph technicians literally stack the deck against their subjects, asking them to pick a card from a deck in which all cards are the same, then informing them that the machine has "detected" their deception.²³ The purpose of tricks such as these is to convince the testee, without actually putting it into words, that the machine is infallible. Other technicians will make the blanket statement that the machine is never wrong. This works to bluff some people, who when they find out that they'll be asked to confirm their statements while hooked up to a "lie detector," break down and confess before the session begins.

Some suggestible people will react positively to the testing itself, with the needles going almost off the chart because the suspect has been led to believe that his stress level will increase if he lies. This allows the technician to draw a clear opinion that the suspect was deceptive, and confront him with it after the test. However, even if the chart tracings are unclear and equivocal, they can still serve to intimidate the suspect during the post-test interrogation.

The post-test interrogation is equally important because it provides a third opportunity to break the suspect. The technician goes over some of the questions with the suspect, never stating outright that the suspect lied, by pointing out that

there is a "problem" with some of his responses. This puts the burden of clearing himself on the suspect, making it harder for him to deny complicity. The critical point about the post-test interrogation is that the technician can use the results against the suspect whether the charts show any objective indication of deception or not.

In a criminal investigation using the polygraph, it's important to work with a sophisticated polygraph technician who understands the realities of the situation and who will cooperate with the investigator. The purpose of a polygraph test is to extract a confession or a damaging admission. By itself, it's not admissible in court, but if it can pry a suspect's mouth open and lead him to disclose damaging evidence that the investigator can verify independently, it can help "make" a case. An example is the murder suspect who breaks down under polygraph testing, and who admits the crime and tells the investigator where he hid the weapon.

There's really no moral objection to using the polygraph as an interrogation tool. The genuinely innocent person is in no danger, because the results can't serve as evidence in court to convict him wrongfully. The suggestible guilty person is open to suggestion, and the polygraph can induce him to confess.

In some cases, a stupid or very suggestible person is open to outright deception. In one case, which has become a legend in its own time, investigators placed wires from a photocopy machine on a suspect's arms. When the suspect gave an answer they didn't like, an officer pushed

a button on the machine, and out came a sheet of paper with "He's lying" on it. This story, which has been attributed to several police agencies in different parts of the country over the years, may be only legend.

The only serious problem is the street-smart suspect who understands his rights, and knows that police cannot force him to submit to a polygraph test. The investigator is thwarted at the outset, and will have to find another method of obtaining the material he needs for his case.

Torture

Another type of coercion is physical torture during interrogation. Slaps and punches are common forms of physical coercion, but sometimes torture takes exotic forms. In 1985 a sergeant and a patrolman at New York City's 106th Precinct used a stun gun on several suspects to induce confessions.²⁴ They were convicted and sentenced to prison. As previously noted, this incident resulted in a lawsuit against the city. Another officer was cleared of charges after six years of delays.²⁵

Stun guns are useful for "curbstone justice" and as interrogation tools, provided officers use them properly. The mistake officers have made in the past is not realizing that stun guns tend to leave characteristic first-degree burn marks on the skin. Pairs of marks spaced the same distance as stun gun electrodes result when applying the stun gun through clothing, because the high-voltage current arcs and burns the skin.

Applying the electrodes directly to exposed skin greatly reduces the possibility of burns because of the direct contact. A further step is wetting the skin first, preferably with salt water. Best of all is conductive jelly, used for electrocardiograms and for electro-shock treatments, obtainable at a medical supply house. Improvising conductive jelly by mixing saturated salt solution with vegetable lubricant, such as "K-Y," is another way to prevent burns.

Whatever the means, it always helps to elicit a confession. At times, however, a suspect doesn't make it into the police station. This is allowable if the suspect's demise doesn't involve the officer in a disciplinary proceeding or a criminal charge. At times, however, there is a mistaken shooting which can shatter a career. Taking an innocent life is bad enough. Being prosecuted, with its severe effects on the officer's family, is worse. This is why we'll examine alibi guns next.

Notes:

1. *Arizona Republic*, August 5, 1992
2. *The Mugging*, Morton Hunt, NY, Signet Books, 1972, pp. 121-122.
3. *Ibid.*, p. 127.
4. *Interrogation: Techniques of the Royal Canadian Mounted Police*, Anonymous, Boulder, CO, Paladin Press, 1991, pp. 47-48
5. *Ibid.*, p. 49.
6. *Privacy For Sale*, Jeffrey Rothfeder, NY, Simon & Schuster, 1992, pp. 86-88.

7. *Interrogation: Techniques of the Royal Canadian Mounted Police*, p. 12.
8. *Ibid.*, pp. 13-15.
9. *Ibid.*, pp. 42-43.
10. *Merchants of Treason*, Thomas B. Allen & Norman Polmar, NY, Delacorte Press, 1988, pp. 205-215.
11. *Ibid.*, pp. 298-303.
12. *Interrogation: Techniques of the Royal Canadian Mounted Police*, p. 55
13. *Ibid.*, p. 30.
14. *Ibid.*, p. 37.
15. *Ibid.*, pp. 52-54.
16. *Interrogation*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987, p. 70.
17. *Badge of Betrayal*, Joe Cantlupe & Lisa Petrillo, NY, Avon Books, 1991, pp. 73-85.
18. Associated Press, January 14, 1991.
19. *A Tremor in the Blood*, David Thoreson Lykken, NY, McGraw-Hill, 1981, p. 30.
20. *Ibid.*, pp. 55-62.
21. *Maricopa County Attorney's Office Investigative Report, Mesa Police Department Internal Affairs Complaint No. 92-24 and 92-53*. Prepared by Paul W. Ahler, Deputy Maricopa County Attorney, Chief, Special Crimes Division.
22. *Lie Detection Manual*, Dr. Harold Feldman, NJ, Allison Press, 1982, p. 28.
23. *Ibid.*, p. 161.
24. *Police Marksman*, July/August, 1985, p. 24
25. *Law Enforcement News*, NY, John Jay College of Criminal Justice, June 15/30, 1991, p. 2.

7

Alibi Guns: Uses And Abuses

Another area of rule-bending is the "alibi gun," or "throw-down knife," used to justify a mistaken shooting. The alibi gun should be untraceable to the officer, of course, which precludes his dropping his back-up gun at the scene. Some officers, when they confiscate a weapon from a suspect they do not arrest, keep the weapon for themselves because they know that it can serve to justify an arrest or a shooting in certain circumstances.¹

It's easy for an officer to obtain an alibi gun by confiscating it from a suspect. Often, a street-

smart suspect understands the officer's motives, but also understands that it's in his best interest to play along to avoid criminal charges.

An officer who obtains an alibi gun may be causing complications for himself if the gun's previously been used in a crime. Some suspects aren't too dismayed by losing their guns to an acquisitive police officer because this provides a one-way gate for losing the evidence. If the officer is later discovered to have the gun by his superiors, he can't point the finger at the suspect from whom he confiscated it because this would implicate him in an illegal cover-up.

The same danger exists when buying a firearm from an illegal source or from a casual acquaintance. It isn't easy to trace a gun's provenance without making official waves, and a gun with a record can be incriminating in its own right. If it's on a list of stolen property, mere possession can bring serious consequences.

William Jordan, a former U.S. Border Patrolman, describes the rationale behind the alibi gun in his book, *No Second Place Winner*.² Jordan relates a hypothetical case of a person who matches a suspect's description, and who reaches in his pocket for a handkerchief after being challenged by an officer. The officer, thinking that the person's reaching for a weapon, blows him away. It's worth noting that he wrote this book after he'd retired. It would be unwise for any police officer to endorse the use of an alibi gun while still serving, as his words might return to haunt him in court one day.

New York's Harlem riots of 1964 began when a police officer shot a Black youth, stating that the youth had attacked him with a knife. There was a knife on the scene, but some residents alleged that the officer had thrown the knife down after shooting the suspect. A police investigation cleared the officer, but this did not satisfy critics, who felt that the investigation had been a whitewash.

Many police agencies make it somewhat difficult for an officer to carry an alibi gun. The rules state that any firearm carried by a police officer must be department approved, inspected, and registered. If an officer wants to carry a "back up" gun, for extra protection in case his weapon malfunctions or is taken by a suspect, he must submit it for inspection by the departmental armorer, and must "qualify" with it. "Qualifying" means that he must demonstrate his proficiency with it on the firing range.

This still doesn't stop the officer from carrying an alibi gun. It merely prevents his using his back-up weapon to alibi a wrongful or mistaken shooting. Most police officers carry patrol cases with them to hold the forms, statute books, extra handcuffs, and other paraphernalia they need on patrol. The patrol case is normally beside them, on the front seat of the car. Inside can be a small handgun wrapped in a rag or plastic bag, in case of need.

What's not obvious to people, except police officers, jurists, and lawyers, is that a firearm isn't necessary to justify a shooting. A knife will do as well at close ranges. This includes distances out to 21 feet. Since most police-felon shootings take

place at close ranges, a knife or club will serve as an alibi weapon.

Another misconception is that the alibi weapon must be clean of the officer's fingerprints. Not necessarily. Normal police practice is to remove any weapon from a suspect's hand, even if he's down and apparently incapacitated. This is a prudent safeguard against a suspect's reviving and resuming his aggression. A pistol or knife may well have the officer's fingerprints on the outside. The only caution the officer must observe when preparing an alibi gun is not to have his prints on the ammunition. In fact, it's not even necessary to have the handgun loaded, because the officer is not obligated to spot a suspect the first shot in an affray.

Notes:

1. *City Police*, Jonathan Rubinstein, NY, Ballantine Books, 1973, p. 289.
2. *No Second Place Winner*, William Jordan, privately printed, 1965, pp. 15-17.

8 Obtaining Evidence

There are several classes of evidence that can help or make a case. Verbal evidence is statements from victims, witnesses, and suspects. Documentary evidence is paperwork, such as forged checks, that help establish guilt. Physical evidence takes in fingerprints, fired bullets, tire tracks, and other types of tangible evidence of crime.

Experienced investigators value physical evidence because they know that it increases the chances of clearing and prosecuting a case.¹

Physical evidence is so valuable that, as we'll see, officers sometimes generate it themselves.

Wiretapping

Wiretapping, bugging of premises, and other electronic surveillance techniques have had their ups and downs. They've been legal at times, totally illegal after some court decisions, and legal with a warrant in other jurisdictions.

Police officers sometimes use illegal methods in conducting investigations. Officials of the Missouri Highway Patrol placed illegal wiretaps in internal investigations during the 1980s. Col. C. E. Fisher, Missouri Highway Patrol Superintendent, called the wiretaps a "stupid" way to obtain information.²

Wearing A Wire

A "wire" is a slang term for a microphone or recording device hidden on the person. There are several varieties, all battery-operated, and their purposes range from monitoring a deal for the undercover officer's protection to securing and recording damaging admissions for prosecution.

A simple radio mike transmits to a nearby receiver and/or recorder. A tape recorder does not transmit, but records for as long as the tape cassette lasts. The microphone, which is necessary for both transmitter and recorder, has to be where it will pick up sound with minimal interference. It may be disguised as a tie clip,

button, etc., but it cannot be concealed under clothing. Clothing masks and muffles sound, and its rustling generates interference which can overpower the sound to be recorded.

The transmitter or recorder can be almost anywhere. Two favorite places are in the small of the back, and in the groin area. Because of cultural sensitivities to searching the groin area, this is fairly safe, but not against someone who knows the trick and orders a strip search. Wearing a wire has become almost ineffective against experienced organized-crime figures because they're both sophisticated and cautious. If they have the slightest suspicion, or feel that they don't know their co-conspirator well enough, they'll insist on a full body search before getting down to business.

Undercover officers using recorders behave in a certain way, asking the target to be very explicit in his statements, and to recite or repeat the obvious. This can tip off the subject that he's being maneuvered into making damaging admissions.

Countermeasures used by street-smart criminals to avoid having their conversations recorded and used against them include:

- Caution in discussing sensitive topics with casual acquaintances.
- A full search of anyone who might be wearing a recorder or transmitter. It's important to note that wire-wearers favor the small of the back and the crotch.
- Discretion while using the telephone. This is standard practice among organized crime

leaders, who always assume that any line may be bugged.

- Never holding any sensitive discussion in the other person's premises or car, which might have a well-concealed bugging device.
- Insisting that any meeting or discussion of sensitive topics be moved from the originally planned location, because of the possibility that the premises may contain bugs. Even public places can be dangerous this way, because of "shotgun mikes" and other listening devices.

Notes:

1. *Forensic Evidence and the Police, The Effects of Scientific Evidence on Criminal Investigations*, National Institute of Justice Report, 1984, pp 69-70.
2. *Law Enforcement News*, NY, John Jay College of Criminal Justice, December 15, 1991, p. 5.

9

Manipulating Evidence

Physical evidence is the strongest way to "make" a case. At times, physical evidence you may need simply isn't available, and it's necessary to fudge to obtain a conviction or confession. In other instances, the evidence is solid, but it's necessary to shade the truth regarding its acquisition. This is, strictly speaking, perjury, but it happens every day.

Perjury has two main uses; to justify an affidavit for a search warrant, and to supply "probable cause." Police officers often use information obtained from snitches in their

warrant affidavits. Often, this information is impossible to check out before making the affidavit, but the officer will perjure himself and state that he did check it carefully.¹

Occasionally, this practice kicks back at the officer. A Boston, Massachusetts, detective received a sentence of five years on probation for inventing a fake informant in a warrant affidavit. During the raid, the convicted officer's partner was shot to death. A consequence of the fudging of the affidavit was that much of the evidence that would have served in convicting the suspect who shot the officer was thrown out.²

It's common to fudge testimony to establish probable cause, thereby justifying an otherwise illicit search. An officer who takes a drug user out of his car and finds a baggie of marijuana in the glove compartment or under the seat will testify that he smelled marijuana smoke, or saw a few marijuana seeds on the front seat.

Police frustration at not being able to make good cases against people they know are guilty sometimes spills over into illicit acts. Planting evidence is one act that frustrated investigators use. This goes by various names, depending on the locale. It's called "farming" in Philadelphia, and "flaking" in New York.

The morality of planting evidence is as clear as its illegality. The simple fact is that most crimes do not result in clearance, and habitual offenders "get away with it" until they are apprehended. Investigators who know that a suspect is guilty may have no moral problem with helping their case along with illicit means.

It's one thing to "frame" an innocent person, and another to construct a case against someone with many prior arrests and convictions. Experienced investigators use two rules of thumb to form snap judgments of guilt or innocence.

The first relates to past behavior. A person with a record of theft convictions is more likely to be guilty than someone with no "priors." The other takes in immediate circumstances, including opportunity and motive.

Any officer who plants evidence risks his career, and even his freedom. The Chief of San Juan Bautista, California, was convicted of conspiracy and falsifying evidence on July 14, 1990. This related to a 1988 case in which he added marijuana to a quantity of seized drugs so that he could increase the charge from a misdemeanor to a felony.¹

Sheriff's officers in Maricopa County, Arizona, raided a suspect's home seeking illegal drugs. The officers planted a marijuana bush in the suspect's yard while other deputies were interrogating him inside. Then they brought him out to see it, in an effort to make him think they had solid evidence against him.

On September 19, 1985, Maricopa County Sheriff's officers conducted a raid on the home of Billy Roy Brogdon, alleged to have been cultivating marijuana in his home. Officers planted marijuana plants on a tilled patch on Brogdon's property, then brought him out to see it in an effort to make him confess. This particular effort failed, because Brogdon was never prosecuted, and later unsuccessfully sued the sheriff and his

deputies.⁴ As we'll see later, it would have been better for the officers to have had an informer or agent-provocateur working for them plant the marijuana to provide them deniability.

Fingerprints

Many people, including some police officers, still believe the myth that it's impossible to fabricate fingerprint evidence. Not so. The modern photocopy machine makes it easy, because it uses fine powder, known as "toner," to reproduce the image. The toner clings to the image on an electrostatic drum, and a heating element fuses the toner to the paper. The trick is to place a suspect's fingerprint card on the platen and make a copy of it, but with the heater disconnected. This leaves a non-fused image on the paper copy, and it's possible to "lift" one of the non-fused fingerprint images with tape.

Obtaining Contraband

Obtaining material for use as "evidence" isn't very difficult. In many busts, it's possible to divert a quantity of drugs or other material for later use. Some police officers, especially narcotics officers, do not turn in all the material they encounter. Some reserve a small stash to use to pay informers. Some states, for example, now have laws allowing officers to preserve only a small sample of illicit material while destroying the rest, if the amount is too large and unwieldy.

to transport and store until the trial. An officer can withhold enough to serve as a supply for other purposes. The rationale is that if an informer is addicted, it's better to pay him with confiscated drugs than to give him taxpayers' dollars with which he'll patronize the illicit drug trade. Secreting a private stash of drugs is highly illegal, and paying an informer in this currency is also against the law, but it often happens.

The officer doing this is usually on his own, and his agency will disown and discipline him if it comes to light. A Phoenix, Arizona, officer was suspended without pay for 40 hours for conducting illegal searches and paying informers with drugs. The fall-out from this case was the resignation of two other officers and dismissal of a third. These officers set up drug buys, then allowed their snitches to keep the drugs as payment.⁵

Evidence and Leads

Illegally obtained evidence is not admissible. However, inadmissibility doesn't preclude its usefulness. A break-in can provide leads to where it's possible to obtain evidence legally. Working a "deal" with a suspect, and even interrogation without reading his rights, can produce information useful to the investigation.

An important point for experienced investigators to understand is that even a weak case with planted evidence can still result in jail time for the offender. Many accept plea-bargains

to avoid the risk of a longer sentence resulting from a conviction after trial.⁶

This is most common with street criminals who can't afford private attorneys. Over-worked public defenders, knowing that practically all of their clients are guilty as charged, anyway, typically advise them to take a plea. Full-scale trials consume time, and this is the only way public defenders can cope with their heavy case-loads.

Notes:

1. *City Police*, Jonathan Rubinstein, NY, Ballantine Books, 1973, pp. 386-394.
2. *Law Enforcement News*, NY, John Jay College of Criminal Justice, June 15/30, 1991, p. 2.
3. *Law Enforcement News*, July / August 1990, p. 3.
4. *Tempe Daily News/Tribune*, February 25, 1988.
5. *Arizona Republic*, October 20, 1990.
6. *Under Cover: Police Surveillance in America*, Gary T Marx, Berkeley, CA, University of California Press, 1988, pp. 153.

10

Entrapment

"Entrapment" is inducing an otherwise law-abiding citizen to become involved in crime. Although laws vary from state to state, there are general guidelines that distinguish a legitimate undercover operation from entrapment. First, the suspect must have demonstrated a predisposition to commit the crime. A record of convictions for the particular offense is good documentation of this principle. Another point is that the suspect must have repeated the act several times, to show a pattern rather than a single impulsive or random act. Witnesses can be crucial, and having

the suspect commit his crime in front of others helps buttress the case. Finally, the undercover officer must not take part in the crime. Keeping his hands clean is crucial to his credibility.¹

Police "stings" often border on entrapment, and sometimes they clearly cross the line. One such case, conducted by the Maricopa County, Arizona, Sheriff's Office several years ago, shows this clearly.

Two unemployed truckers answered a classified ad. The person who placed the ad, an undercover sheriff's officer, had advertised for a trucker to move a cargo to Texas. The officer met with the truckers in a diner, where he explained that the load was marijuana, and discussed the logistics and fee with them. They agreed to take on the job, and one evening met the officer at a warehouse in Mesa, Arizona, to load the cargo. Just before the truckers reached the freeway on-ramp, sheriff's cars stopped them, and officers made the arrest. The county attorney declined to prosecute, because of the questionable nature of the case, but the two truckers had an arrest on their records.

One type of sting is using an undercover officer to pose as a killer for hire, and to arrest the suspect when he makes the offer. This works because some people are so eager, or so foolish, in going about hiring a contract killer, that they disclose their intentions to casual acquaintances, who in turn inform police. An undercover officer poses as a "killer for hire," and makes the arrest once he obtains the suspect's voice on a hidden

tape recorder, or obtains payment for the projected killing.

Another type of sting is to use an informer to entrap the target. Entrapment is illegal, and if a police officer is the one who conducts the entrapment, it can destroy the case. This is what happened with the two truckers. However, if a third party, working for the police but unknown to the prosecutor and defense attorney, can make the set-up, his role can be so low-profile that he's out of the picture when the arrest comes down and when the case goes to trial. A simple example is the informer who agrees to plant drugs in the target's home or car. In the simplest method of operation, he lays a baggie of marijuana on the seat of the car. Later, an officer walking by just happens to see it lying in plain sight, and this provides probable cause for search and seizure. Alternatively, an officer can stop the car when the target is driving it, and "happen" to see the baggie, giving him cause for an arrest.

The informer can also serve as agent provocateur, someone who induces a person to commit a crime. The informer, not being a police officer himself, need not appear in any official records. He can, however, persuade a target to commit a crime where the police are waiting for him. Officers can relate the incident in a way that makes it appear that they just "happened" to be on the scene when the suspect committed his crime.

One such was the FBI informer who joined "Earth First!", an ecological movement based in Tucson, Arizona. Members admired Edward

Abbey, author of *The Monkey Wrench Gang*, a novel advocating and describing physical destruction of equipment used by corporations despoiling the environment. The FBI agent provocateur persuaded members of "Earth First!" to destroy power lines leading to a nearby nuclear generating plant, and FBI agents were waiting for them.

One successful case of entrapment of a person without a previous record was that of a Florida businessman seeking money to reorganize his football team. A man telephoned him, offering to set him up with investors who would supply the money. A condition of the deal, according to the agent provocateur, was that the businessman supply the investors with cocaine. At first, the businessman refused, but later relented and introduced the agent provocateur to two men who sold him cocaine. This resulted in a conviction and prison term for the target of the investigation.²

Delivering illicit materials to the target of an investigation is another way to use an informer and agent provocateur. Los Angeles officers seeking to make a case against anti-war activists arranged for their agent provocateur to deliver a case of hand grenades to their home. This led to their subsequent arrest for possession of the grenades.³

Undercover operations also border on entrapment, and often cross the line because they offer many opportunities for officers to "set up" a suspect. This type of set-up is very flexible, versatile, and safe to conduct because of the

tenuous nature of the link between an informer and his control officer.

An informer/agent provocateur can play a role in planting evidence. The informer can emplace the contraband before arresting officers arrive, to provide the officers with deniability in case of an investigation. Only the leader of the raiding party need know that planted evidence is waiting for discovery.

The important point is to have the informer sign an agreement in which he understands that he is not to break any laws during his service as an informer. The control officer explains to the informer that this is merely a formality, which it is, and that in practice the informer will have a free hand to use whatever methods, legal or illegal, that he and the officer decide to use. The paper only comes into play in case something goes wrong, and the informer's link to the police comes to light. Having this document protects the officer from complicity, as it shows that the informer was operating on his own, without authorization.

At times, law officers conduct entrapment by mail-order, and they have made their cases stick. During the late 1980s, the U.S. Postal Inspectors conducted "Operation Looking Glass," directed against child pornographers. In 1986, law officers raided a Los Angeles film company and secured a list of customers for pornographic films and videotapes. Postal inspectors set up an operation with a mailing address outside the United States, and sent advertisements to people on the film company's customer list. One man they arrested

was Kenneth J. Hendin, of Sarasota, Florida, on a charge of receiving two videotapes of teen-age and pre-teen boys engaged in explicit sexual activity.⁴

Some of the cases built up by postal inspectors have been questionable. One postal inspector corresponded with clients, adopting the sobriquet of "Richard Teninch." He succeeded in enticing a Phoenix man into describing his child molestation exploits, under the guise of soliciting manuscripts for publication in a kiddie-porn anthology.

It's easier to work a sting on obviously criminal enterprises, such as car theft rings. One such operation took place as a cooperative effort between state and federal authorities in New York and New Jersey. Undercover officers bought cars from this ring, which employed professional car thieves who stole vehicles to order. Officers requested late-model luxury cars, which the rings stole and delivered to a warehouse in Carlstadt, New Jersey, which FBI technicians had equipped with hidden video cameras.⁵

A very successful "sting" was the notorious "AZSCAM" Project, which netted several state legislators who accepted bribes from one Joseph Stedino, working for the Maricopa County, Arizona Attorney's Office under the name of "J. Anthony Vincent." Vincent-Stedino passed himself off as a high-living mob personage, and his original task was to insinuate himself into illegal gambling circles in Phoenix. Soon, however, he learned that several state legislators were amenable to selling their votes. Introduced by an intermediary, Stedino approached legislators and

propositioned them in rooms bugged by law officers. He suggested that affluent gambling interests wanted Arizona to legalize casino gambling, and were willing to pay for votes. This resulted in several of them accepting bribes on-camera. Some of these legislators resigned, and some stood trial. Several have served prison time for their offenses.

What was remarkable about the AZSCAM sting was that Stedino was able to play his game for as long as he did. He operated for many months before one legislator he'd approached alerted police. None of the others, even those who had declined his offer, had reported him to police, suggesting that there exists a tolerance of bribery among Arizona legislators. It also suggests that many legislators who were not themselves open to bribery were reluctant to turn in their colleagues who were doing wrong.

Notes:

1. *Undercover Work*, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1986, p. 42.
2. *Under Cover: Police Surveillance in America*, Gary T. Marx, Berkeley, CA, University of California Press, 1988, p. 130.
3. *Ibid.*, p. 134
4. *Tampa Tribune*, April 13, 1988.
5. *Newark Star-Ledger*, January 11, 1992.

11 Pro-Active Enforcement

"Pro-active" policing is in sharp contrast to "reactive" law enforcement. Most police officers are reactive because they respond when a crime is in progress or has been completed. Pro-active policing carries the fight to the enemy, and can forestall criminal activity. Stings, reviewed in the last chapter, are examples of pro-active police work. Here we'll examine more vigorous measures.

One time-honored crime control tactic is to expel undesirables. Traditionally, the town sheriff or marshal confronted street criminals and ordered them to get out of town. Today's litigious civil-

rights climate puts a damper on such active measures, yet they sometimes still take place.

The Los Angeles Police Department has for decades sought to keep organized crime off its turf. During the 1930s and 1940s detectives assigned to the organized crime unit watched train stations and turned back arriving mobsters. If verbal persuasion didn't work, they'd administer beatings to adjust the mobsters' attitudes. During the 1960s, officers would meet arriving mobsters at the airport and make it clear to them that they were unwelcome. By this time, beatings had stopped, and verbal dissuasion was enough to persuade the newcomers to turn around immediately. Darryl Gates, former Los Angeles Police Chief, admitted that such tactics are out of place during the last decade of the 20th Century because of "civil-rights" litigation.¹

Political Investigations

Police agencies often have occasion to investigate politicians and their shortcomings. Even the smallest small-town police chief sometimes has to stop the mayor's son driving drunk down Main Street. At times, it's the mayor himself. In such cases, politics intervenes, and the local officer has to discreetly drive the mayor home. However, in true American-style politicking, the deed goes on deposit in the officer's "favor bank" to be redeemed when he needs it.

Contrary to the protests of liberal civil-rights advocates, investigating city and state politicians is legitimate police work, even if they're not

under suspicion of a street crime. A simple and understandable fact of life is that a mayor, governor, or state legislator is not going to stick up a gas station. There are less risky ways to earn illicit money.

Like other people, some politicians lead double lives. Walter Jenkins, one of President Lyndon Johnson's White House staffers, was arrested in a Washington toilet for homosexuality. This wasn't his first arrest. Massachusetts Congressman Barney Frank's roommate ran a male prostitution ring from the apartment they shared. Many other federal legislators have been involved in scandals relating to alcoholism, illicit sex, financial wrongdoings, etc. From this it's obvious that politicians are prime targets for investigation because they have both the opportunities and propensities for illegal acts.

The Los Angeles Police Department, charged with policing California's most populous city, regularly investigates politicians, entertainers, and other high-profile people because of their proximity to organized crime figures. Politicians are always desirable people to bribe. Movers and shakers behind the scenes are often making private arrangements outside the law. The entertainment industry has a solid record of affiliations with organized crime, and many entertainers are involved in illicit sex or drugs. When an investigation takes place, it necessarily involves the subject's known associates, who may be part of the crime.

There have been recent investigations of Los Angeles Mayor Tom Bradley, Congressmen

Edward Roybal and Mervyn Dymally, Councilman Richard Alatorre, State Senator Art Torres, and others. One author has labeled these "fishing expeditions."² It's clear that such investigations are justified, given the well-documented corruption prevalent in American politics. The alternative is for police to put on blinders and refuse to investigate possible criminal involvement by the high and mighty because they are above the law.

Counter-Insurgency

Police conducting counter-intelligence or counter-insurrection programs generally have more freedom of action than ordinary officers. There may be an "emergency" declared, and a suspension of civil rights and ordinary criminal justice procedures. Also, police in such instances develop a siege mentality, justifying extreme measures.

An important point is that totalitarian secret-police methods are not the monopoly of dictatorships. There have been "killer-squad" hits undertaken by British S.A.S. troopers during the Northern Ireland War in recent years. S.A.S. troopers are a far cry from the conventional unarmed and friendly British "Bobbies," and the British government justified such harsh methods by citing the violence of the Irish Republican Army.

Police methods can become very extreme during "emergencies," when both the police and its government feel that the survival of the nation

is at stake. American anti-war organizations during the Vietnam Era came under surveillance by local police, the FBI, and Army Intelligence, as well as other military organizations. The government's concern was that peace organizations were communist fronts, and they strove to uncover connections with foreign governments. With all that, the Vietnam Era protests and government reactions were relatively peaceful, despite a few unintentional deaths such as the Kent State University shootings. For examples of heavy-handed and lethal police actions, we have to look to foreign shores. The British counter-insurgency in Malaya during the late 1940s provides an example of how a "democratic" Western government and its police organizations can pull out all the stops when the struggle takes place away from home, and the insurgents are non-Caucasians.

Case Study: "The Officer From Special Branch"

Typically, secret-police methods and tactics fall under a cover of deep secrecy, often never to see the light of day. A few accounts surface, usually provided by the victims of the police, but many dismiss their statements as propaganda. The occasional renegade police officer discloses some of the events after his retirement, when he's beyond the reach of agency discipline. Some topics, and some wars, remain hot potatoes decades after their end and anyone who makes state secrets public risks prosecution. This is

especially true in Great Britain, where the 'Official Secrets Act' allows prosecution of anyone who reveals classified information, however obtained.

This is why some British Intelligence officers have gone abroad to publish their memoirs. A recent one was Peter Wright, author of *Spycatcher*, who had his memoirs published in Australia and the United States. Another was the individual who used the pen name 'Tom Lilley,' who appears to have been a British police officer serving during the Malayan insurrection. Lilley published his disclosures in the form of a novel, probably to avoid lawsuits from British police officers who actually served in Malaya and used the methods outlined in Lilley's book. The foreword stated that none of the methods described were actually used by the authorities in Malaya, that all characters are fictional, and that the novel is set in a fictional Malayan state. These multiple disclaimers almost guarantee that the story is thinly disguised fact, and that police tactics and stratagems described reflected reality.³

The first police dirty trick described is the arrest and interrogation of five suspected communist underground leaders. The local head of "Special branch," the British political and secret police, arranged for every adult in the village where the five suspects lived to be interrogated for four minutes each as part of the deception plan. The first of the five suspects to arrive at the police station, however, would undergo a five-hour interrogation, after which he'd be released while police arrested the other four suspects. The

Special Branch head calculated that this would give the impression that the arrests resulted from information provided by the man they'd interrogated and released, and that fear of arrest might stampede other communist guerrillas into trying to escape. A side-effect was that the communists would seek revenge on the man they'd been led to believe had betrayed them. This gruesome prospect did not disturb the head Special Branch officer. His only worry was that there might be no attempt on this suspect's life, which would suggest that his information had been wrong.

The operation went as planned, and several previously unsuspected communists ran into ambushes in trying to sneak out of the village one night. The man whom the police had set up as the putative informer was shot to death at a barbershop, and his killers cut out his tongue to connote that he'd died for informing.

Another trick, undertaken early in the story, was to booby-trap any abandoned communist guerrilla camps British troops discovered. This was better than total destruction upon discovery because it became possible to destroy some guerrillas as well, instead of merely physical property. To lure a communist guerrilla unit into the booby-trapped camp, Special Branch officers arranged for a forged order from the communist high command to reach the leader of a particular guerrilla company. An anti-communist volunteer would bring the note to the communist troops, and to lend realism to the effort, there would be a faked fire-fight with British troops in the area.

The fake communist guerrilla would have a surgical wound in his leg to simulate a bullet wound. The plan worked, and when the guerrillas occupied the camp, British sappers detonated the mines, killing almost all of the communist unit. Their commander, however, escaped unhurt.

The Special Branch devised another plan to capture the guerrilla leader by blackmailing his brother, a schoolteacher who kept a mistress on the side. They persuaded the brother to lure the guerrilla commander into a trap, and this was where Special Branch officers and British troops captured him.

British troops occasionally discovered guerrilla supply dumps, and this gave Special Branch further opportunities. The plan was to sabotage or adulterate communist supplies, instead of destroying them. Special Branch officers knew that one guerrilla leader was diabetic, and when they discovered a stockpile of insulin, they diluted the liquid in the vials so that the leader would fall ill. This was preferable to inserting poison, which would kill him. The reasoning was that, if the guerrilla leader died, the communist high command would merely replace him. By diluting his insulin, they'd keep him partly incapacitated and less able to carry out his duties.

Another wrinkle in the sabotage plan was to contaminate communist rice stockpiles with bamboo hairs. These are very fine, and almost invisible. When ingested, they become embedded in the stomach walls because of their fish-hook

shape, and cause chronic inflammation which is practically incurable.

Starting Wars

A police intelligence unit can sometimes take advantage of an opportunity to instigate a gang war between rival criminal factions. If there already exists a dispute over territory, sharing the trade, or other issues, a careful 'hit' made to look like the handiwork of a rival gang can provoke reprisals.

The crucial factor is that tension and distrust between the two target groups be so high that demands of guilt won't be credible. With both sides poised for war, it doesn't take much to light the spark.

Notes.

- 1 *L.A. Secret Police*, Mike Rothmuller and Ivan Goldman, NY, Pocket Books, 1992, pp. 143-144
- 2 *Ibid*, pp. 156-157
- 3 *The Officer From Special Branch*, Tom Lilley, NY, Doubleday & Company, Inc., 1971, 'Foreword' p 7

12

Finale

Methods such as these help police fight fire with fire. Our outnumbered police officers, confronted by street smart gangsters who openly flout the rules and know all the tricks, need an edge to avoid being swamped by dangerous law-breakers. At times, breaking the rules and using extra-legal methods provide the needed edge.

13

For Further Reading

A Speeder's Guide to Avoiding Tickets, Sgt. James M. Eagan, N.Y.S.P. (Ret.) NY, Avon Books, 1990. *This is a very easy-to read guide to traffic ticket survival, written by an experienced state trooper.*

Badge of Betrayal, Joe Cantlupe & Lisa Petullo, NY, Avon Books, 1991. *This book recounts the story of an investigation by police into the deadly conduct of another person wearing the badge. It tells of how investigators finally apprehended the*

144 Dirty Tricks Cops Use

officer who went bad, using common investigative methods, including the good cop/bad cop technique.

By Way of Deception, Victor Ostrovsky and Claire Hoy, NY, St Martin's Paperbacks, 1991
The author uncovers the successes and especially the failures of the Israeli spy and covert action network. These accounts allow us to see what can go wrong in secret actions, and to draw lessons from other people's failures.

City Police, Jonathan Rubinstein, NY, Ballantine Books, 1973. *The author rode with Philadelphia police officers until they got so used to him that he became part of their background, and they acted as if he wasn't there. This provided a crucial and eloquent insight into how cops really think and act.*

Criminal Victimization in the United States, 1990, U.S. Department of Justice, Bureau of Justice Statistics, February, 1992 Report NCJ-134126. *This report is the alternative to the FBI Uniform Crime Reports, and is based on a sampling of Americans across the country, not just those who report crimes to police. One surprising finding of this series is that the trend in crime rates has been downward since 1973, although reported crimes have tended to increase. Apparently, although there are now somewhat*

fewer crimes, somewhat more people are reporting them.

Family Of Spies, Pete Earley, NY, Bantam Books, 1988. *Family of Spies provides a look at how FBI counter-espionage agents conduct investigations. Reading between the lines shows that there are many spy cases incomplete or undetected.*

Interrogation, Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987. *A good book that provides a comprehensive, no-holds-barred look at what really happens in interrogations.*

Interrogation: Techniques of the Royal Canadian Mounted Police, Anonymous, Boulder, CO, Paladin Press, 1991. *This text provides many tricks and deceptions for cajoling a confession from a suspect.*

L.A. Secret Police, Mike Rothmiller and Ivan G. Goldman, NY, Pocket Books, 1992. *The authors tell of the secret methods used by a secret unit of the LAPD. Some methods are unattractive, but the LAPD has had to deal with some very unattractive and unsavory lawbreakers.*

Law Enforcement News, NY, John Jay College of Criminal Justice. *This is the most objective law enforcement publication in the country because it's not connected with any police agency and does not run advertisements by suppliers of police*

equipment. The editorial slant is on the liberal side, but the reporting is both accurate and comprehensive.

Merchants of Treason, Thomas B. Allen & Norman Polmar, NY, Delacorte Press, 1988. *This book also provides a look at the no-holds-barred world of counter-espionage, where a variety of dirty tricks are both justifiable and legal.*

Privacy For Sale, Jeffrey Rothfeder, NY, Simon & Schuster, 1992. *The world of computer espionage and information-gathering is widespread and frightening. In fact, the biggest violators are not police agencies, who have their hands too full with dangerous lawbreakers to bother peeping at innocent citizens, but commercial data-collectors, who gather a variety of privileged information about Americans for crassly commercial purposes.*

The FBI-KGB War, Robert J. Lamphere and Tom Shactman, NY, Berkley Books, 1987. *Lamphere's book gives us an inside view of how the counter-espionage effort of the 1940s and 1950s was run by the FBI. The raw information is both startling and enlightening.*

The Mugging, Morton Hunt, NY, Signet Books, 1972. *This account of a mugging also provides chapters on topics such as police interrogation techniques.*

The Officer From Special Branch, Tom Lilley, NY, Doubleday & Company, Inc., 1971. *This is a fictional representation of real-life events, with locale and author disguised to prevent reprisals.*

Sourcebook of Criminal Justice Statistics — 1990, Washington, DC, U.S. Department of Justice, Bureau of Criminal Justice Statistics, 1991. *Each annual in this series provides a comprehensive look at the crime picture in this country, and an interesting outline of various branches of the criminal justice system.*

The Squad, Michael Milan, NY, Berkley Books, 1992. *The Squad is a surprisingly frank and unofficial look at how a low-profile police intelligence unit really operates. This book isn't a glorification of the unit, but an account of both successes and failures, with the emphasis on how personalities and politics often impede the unit's effectiveness.*

Surreptitious Entry, Willis George, Boulder, CO, Paladin Press, 1990. *George's book is a classic on black bag jobs, and how the government used them against both civil lawbreakers and foreign agents.*

A Tremor in the Blood, David Thoreson Lykken, NY, McGraw-Hill, 1981. *This is the authoritative book on the polygraph and other gadgets and gimmicks touted as "lie detectors." The author also*

148 **Dirty Tricks Cops Use**

deals with honesty tests and shows how and why they are ineffective.

Under Cover: Police Surveillance in America, Gary T. Marx, Berkeley, CA, University of California Press, 1988. *Under Cover* is a collection of accounts of how police surveillance methods go wrong, often citing abuses, and how not to do it. This is a good text on how not to do it.

Index

- Aerosols, 43
- Affidavits, 55, 60, 61, 117, 118, 119
- Agent-provocateur, 60, 120, 125, 126, 127
- Alibi gun, 109, 110, 111, 112
- Alibi weapon, 112
- Ambushes, 18, 48, 137
- American Civil Liberties Union, 73
- Arizona v. Fulminante, 100
- Army Intelligence, 135
- Arresting felony suspects, 31
- Arrests, 1, 3, 4, 5, 32, 34, 119, 137
- Artificially depressed speed limit, 14
- Avoiding injury, 32
- AZSCAM, 128, 129
- Bagman, 58
- Ballentyne, Del, 102
- Bank records, 64
- Baton, 43, 44
- Beatings, 9, 39, 40, 41, 132
- Bill of Rights, 79
- Biting, 88
- Black bag jobs, 55

150 **Dirty Tricks Cops Use**

- Blackmail, 84, 138
- Blame Society Ploy, 86
- Blame The Victim, 86
- Bodyguards, 43, 48
- Booby-traps, 58, 137
- Boy Scout mentality, 3
- Bradley, Tom, Los Angeles Mayor, 133
- Broderick, "Broadway John ny," 41
- Brogdon, Billy Roy, 119
- Brutality, 43, 81
- Buddhist Temple Murders, 78
- Bureau of Justice Statistics, 9
- Byrne, Patrolman Eddie, 46

- Car theft rings, 128
- Career criminals, 5, 81
- Chemical agents, 43
- Chin, Larry Wu-Tai, 90
- CIA, 90
- Circumventing Miranda, 79
- City directories, 63
- Clearance rates, 1
- Confessions, 1, 36, 73, 75, 76, 77, 78, 79, 80, 81, 82, 85, 86, 87, 92, 93, 94, 96, 99, 100, 101, 104, 105, 106, 117, 145
- Confiscation, 35, 59, 109, 110, 121
- Contempt of cop, 26
- Control officer, 127
- Cop-haters, 42
- Cop-killers, 45
- Correctional Association of New York, 25
- Counter-espionage, 55, 145, 146
- Counter-insurrection programs, 134, 135
- Credit card records, 64
- Crime prevention, 2
- Curbstone justice, 40, 41, 105

- Damaging admissions, 104, 114, 115
- Deceptions, 32, 52, 81, 89, 91, 95, 103, 104, 136, 144, 145
- Dirty Harry, 8, 44
- Discretionary justice, 34
- Divide and Conquer, 82
- Documentary evidence, 113
- Double agent, 46, 66, 88, 90
- Dropping a dime, 54
- Dropping the Charges, 91, 92
- Drug dealers, 3, 34, 39, 58
- Dudley Do-rights, 48

- Eagan, Sergeant James, 20
- Earth First!, 125
- Electronic intelligence files, 73
- Electronic surveillance, 31, 114
- Employee theft, 85
- Entrapment, 1, 55, 123, 124, 125, 126, 127
- Exaggerating the charges, 80
- Excessive force, 39, 42

- Fake or phantom file, 92
- Falsifying evidence, 119

- FBI, 1, 7, 32, 36, 47, 48, 68, 85, 87, 88, 90, 126, 128, 135, 144, 145, 146
- FBI agents, 32, 33, 36, 68, 87, 90, 126
- FBI informer, 125
- FBI statistics, 1
- FBI Uniform Crime Reports, 1, 9, 24
- Federal Witness Protection Program, 68
- Felony warrant arrests, 32
- FinCEN (Financial Crimes Enforcement Network), 70
- Firearms, 49, 50, 78, 110, 111
- Flattery, 87
- Fugitives, 28, 29, 36, 37, 69
- Fugitive detail officers, 34
- Full body search, 115
- Fulminante, Oreste, 100, 101
- Gang colors, 27
- Gates, Darryl, former Los Angeles Police Chief, 38, 132
- Good cop/bad cop technique, 97
- Graymail, 83
- Guerrillas, 137, 138
- Gypsy cab operation, 35
- Habitual offenders, 118
- Harlem riots, 111
- Heavy-duty felons, 3
- Heavy-duty offenders, 3
- Heavy-duty suspects, 66
- Hendin, Kenneth J., 128
- High-crime areas, 25, 34
- High-level stock frauds, 25
- High-profile cases, 77
- Immediate confession, 80
- Incriminating information, 89
- Incriminating statement, 17
- Inducing a suspect to attack, 44
- Informal deportation, 37
- Informers, 1, 35, 48, 55, 63, 64, 65, 66, 67, 68, 69, 84, 87, 99, 100, 101, 103, 120, 121, 125, 126, 127, 137
- "Innocent people have nothing to hide," 96
- Internal Revenue Service, 64, 69, 70, 84, 85
- Interrogating, 119
- Interrogation, 24, 44, 77, 78, 79, 80, 82, 83, 87, 89, 96, 98, 99, 103, 104, 105, 106, 107, 119, 121, 136, 145, 146
- Irish Republican Army, 134
- "J. Anthony Vincent," 128
- Jordan, William, 110
- Killer-squad, 134
- King, Rodney, 9, 38, 43
- Laser beam, 16
- "Let's Make a Deal," 81, 91
- Lilley, Tom, 136, 146
- Los Angeles Police Department, 38, 132, 133, 145
- Maricopa County Arizona Sheriff's Office, 78, 124

152 Dirty Tricks Cops Use

- Marijuana, 56, 118, 119, 120, 124, 125
- Mind game, 95
- Minimizing the Charges, 93, 94
- Minor offenders, 3
- Minor offenses, 2
- Miranda Warning, 79, 96, 98
- Motorists, 10, 14, 18, 72, 97
- Mugging, 106, 146
- Murder, 1, 24, 47, 48, 78, 93, 94, 104
- 'Mutt and Jeff' technique, 97
- Narcotics, 50, 57, 59, 89
- Narcotics officers, 120
- National Crime Victimization Survey, 9
- National Institute of Justice, 2, 116
- National Security Agency, 87
- Neighborhood Watch, 2
- New police officer, 3
- Nightsticks, 38, 40, 41
- Northern Ireland War, 134
- Office of Technology Assessment, 102
- Officer-involved shooting, 44, 45
- Operation Looking Glass, 127
- Organized crime, 42, 45, 47, 132, 133
- Organized crime figures, 34, 45, 115, 133
- Organized crime unit, 132
- Outstanding warrants, 28
- Overt execution, 49
- Parole, 25, 66, 69
- 'Pay-back time,' 38
- Paying informers, 5, 121
- Pelton, 87, 88, 89, 91
- Phantom charge, 93
- Photocopy machine, 104, 120
- Physical evidence, 37, 42, 45, 78, 113, 117
- 'Pizza man' trick, 33
- Planting drugs, 125
- Planting evidence, 5, 54, 55, 56, 59, 118, 119, 121, 127
- Planted marijuana plants, 119
- Playing one suspect against another, 82
- Plea-bargains, 75, 121
- Police-felon shootings, 111
- Political Investigations, 132
- Polygraph, 14, 101, 102, 104, 105, 147
- Polygraph technicians, 103, 104
- Postal inspectors, 128
- Private attorneys, 122
- Private investigators, 70, 84
- Private security agencies, 3
- Pro-active police work, 131
- Probable cause, 53, 54, 117, 118, 125
- Probation, 25, 97, 118
- Professional courtesy, 12
- Prosecution, 9, 45, 58, 59, 76, 82, 83, 89, 90, 99, 114, 135, 136
- Psychological ploys, 87, 91
- Public defenders, 59, 60, 122

- Public relations, 2
- Quotas, 17
- Radar ambush, 14
- Radar detectors, 15
- Radar gun, 15, 16
- Radio mike, 114
- Reported crimes, 9, 144
- Resisting arrest, 19, 25, 37
- Revenue enhancement, 12, 13
- "RICO" (Racketeer Influenced and Corrupt Organizations), 59, 60
- Rock houses, 58
- Salami-slicing, 85
- Shaffer, Chief Robert E., 12
- Search and seizure, 51, 53, 54, 125
- Search warrant, 48, 53, 55, 60, 61, 117
- Secrecy, 70, 72, 73, 135
- Secret-police methods, 134, 135
- Sharing the guilt, 85
- Situational Awareness, 18
- Situational offenders, 76
- Slush fund, 47, 73
- Sobell, Morton, 36
- Social Security Administration, 69
- Sociopaths, 3
- Soviets, 32, 87, 89, 90
- Special arrest teams, 33
- Special Branch, 135, 136, 137, 138
- Special squad, 47
- Speed traps, 10, 13, 15, 18
- Station, Cherie, 102
- Stedino, Joseph, (J. Anthony Vincent), 128
- Street execution, 45
- Street justice, 26, 40, 41
- Street-fighter mentality, 26
- Street-savvy officer, 26
- Street-smart career criminals, 2, 3, 5, 26, 29, 77, 81, 82, 109, 115, 141
- Street-smart cop, 8
- Strip search, 115
- Stun gun, 105
- Subtle threats, 96
- Surreptitious entry, 55, 56, 58
- Surreptitious search, 54
- Surveillance, 29, 30, 57, 91, 96, 122, 129, 135, 148
- Surveillance team, 31
- Sympathy ploys, 77, 85
- Tape recordings, 98
- Targeting repeat offenders, 51
- TECS II (Treasury Enforcement Communications System), 70, 71
- Telephone company records, 64, 84
- "The French Connection," 30
- Throw-down knife, 109, 111
- Trading up, 66, 67, 76
- Traffic offenders, 2
- Traffic stops, 19, 25, 33
- Traffic tickets, 4, 17, 26, 143
- U.S. Postal Inspectors, 127

DECEPTION DETECTION



WINNING THE
POLYGRAPH
GAME

JOHN B. ESTERLINE

*Deception Detection:
Winning the Polygraph Game*
by Charles Clifton

Copyright © 1991 by Charles Clifton
ISBN 0-87364-621-5
Printed in the United States of America

Published by Paladin Press, a division of
Paladin Enterprises, Inc., P.O. Box 1307,
Boulder, Colorado 80306, USA.
(303) 443-7250

Direct inquiries and/or orders to the above address.

All rights reserved. Except for use in a review, no
portion of this book may be reproduced in any form
without the express written permission of the publisher.

Neither the author nor the publisher assumes
any responsibility for the use or misuse of
information contained in this book.

CONTENTS



CHAPTER ONE	
Polygraph History	1
CHAPTER TWO	
Why Be Concerned about Polygraph Tests?	11
CHAPTER THREE	
The Instrument and the Examiner	25
CHAPTER FOUR	
The Tests	35
CHAPTER FIVE	
Countermeasures	57
CHAPTER SIX	
The Day of the Test	77
CHAPTER SEVEN	
Beyond the Polygraph: Other Abuses	99
CONCLUSION	129
APPENDIX A	
Polygraph Do's and Don'ts	131
APPENDIX B	
Polygraphers' Favorite Verbal Ploys	135
APPENDIX C	
Polygraph Validity Statement	139
GLOSSARY	141

ACKNOWLEDGMENTS



The author wishes to thank Andee, Paul, and Bev for their help and friendship during the good and the bad times, and Adam for supplying the motivation.

CHAPTER ONE

POLYGRAPH HISTORY



*"We live under a
king who hates
deceit, a king whose
eyes see into every
heart and can't be
fooled by an
impostor's art."*

—from Moliere's
Tartuffe, first
performed in 1699

LIE DETECTION THROUGH THE AGES

Why do people lie? There are, of course, a variety of answers to this question. At times we may lie in order to stay out of trouble. ("I swear I didn't cheat on that math test!") We may lie just to be polite. ("Oh, thank you for the lovely birthday present! I've always wanted a Day-Glo on black velvet painting of *The Last Supper*. Now I've just got to find a place to put it.") Sometimes we lie just to avoid a confrontation and save face. ("The check is in the mail.")

Basically, though, we lie because we are human. Situations that demand an immediate course of action are always confronting us. The small child, for example, is caught with his hand in the cookie jar after being told not to do so repeatedly. In a split second, he must decide whether to confess

and suffer the consequences (perhaps a spanking), or to tell a lie and extricate himself from his dilemma. ("But Daddy, I was getting this cookie for you!") Similarly, adults will resort to lying when we believe it will serve our best interests. How many of us can say that we have never fibbed about a nonexistent "previous engagement" in order to get out of an invitation to what will undoubtedly be the world's most boring dinner party?

Because of this seemingly natural predisposition we have toward lying, there have been those among us who have attempted to develop elaborate systems and electronic gadgets to "cut through all the bull" and "scientifically" determine whether an individual is really telling the truth. Perhaps the first recorded instance of an individual actively seeking to detect the truth among his contemporaries was Diogenes of Sinope (412?-323 B.C.), who searched all of Athens with a lighted lamp (even in broad daylight) to find a good and honest man. It is not known whether he ever found one, but he seems to have set the precedent for future generations to try their hands at distinguishing the honest from the dishonest.

The ancient Hindus devised a rather ingenuous method for lie detection based upon a physiological principle. Guilt or innocence was determined with a bowl of rice. The suspect was required to chew on a mouthful of rice and then spit it out. The Hindus theorized that a guilty individual, being more fearful of the test, would suffer from a dry mouth. Consequently, he would be unable to spit out the rice because it would stick to his tongue and mouth. An innocent person, on the other hand, would have no trouble in spitting out the rice because he would not have a guilty conscience.

A variation of this technique was used by the Roman Catholic Church during the Inquisition to test clergy for supposed transgressions. The cleric was

forced to chew on bread and cheese to see whether he could swallow it. Perhaps the most gruesome of these "saliva" tests was devised by the Arab Bedouins of the Middle Eastern and North African deserts. In their version, conflicting witnesses each had to lick a hot iron; the one whose tongue was burned was thought to be lying.

Other early forms of lie detection were similarly based on differing types of physiological phenomena. Liars were regularly "exposed" by the frequency or amount of their perspiration, the quickness of their pulse, or the degree to which they blushed (or failed to blush) when accused of a crime. And if these methods did not work, there was always the rack, the drowning chair, and a variety of other tortures or trials by ordeal. These methods were considered acceptable and reliable in their day, but an unpleasant drawback was that innocent victims tended to die or be physically disabled in the process of being tried.

W.M. Marston

William Moulton Marston is probably the man most qualified to carry the title "father of modern-day polygraphy," for it was Marston who believed he had found a specific physiological response emitted during the act of lying. Although this claim is constantly challenged and hotly debated today, Marston, in his early excitement, proclaimed that the "long, futile search" for an empirical method of detecting deception was finally over. He publicized his new device far and wide, and possibly was the first individual to use the phrase "lie detector."

He claimed that with the lie detector, he could "read hidden thoughts like print on a page." But there were those who argued that some of Marston's uses for the polygraph were trivializing the industry. One such stunt involved using the polygraph as a marriage

counselor by comparing a wife's responses first to a kiss by her husband and then to a kiss by a total stranger. It was only a matter of time before mainstream polygraphers began to openly attack Marston and his views in order to discredit him. The attacks must have worked because Marston faded from the polygraph scene and found other outlets for his creativity. Today, he is best remembered as the creator (under the name Charles Moulton) of the comic book character "Wonder Woman," a heroine who could compel people to tell the truth by lassoing them with her magical golden lariat.

John Larson

John Larson is a noteworthy individual in the history of polygraphy because, despite a tremendous initial success, he always maintained a healthy skepticism with regard to the machine and its supposed powers. As a police officer, Larson was aware of Marston's findings and their possible impact on police interrogations. It is believed that Larson thought of the polygraph as a humane form of interrogation that could be used as a favorable alternative to the all-too-common practice of beating a confession out of a suspect.

While conducting experiments on changes in blood pressure and respiration during questioning, Larson had the opportunity to put his technical skill to a practical test. A local store was suffering from shoplifting. The shopkeeper believed he knew the dormitory where the shoplifter resided but could offer no further assistance. After assembling a series of questions relevant to the crime, along with some neutral, or irrelevant, questions (soon to be called the R/I test—see Chapter 4), Larson interrogated every resident of the dormitory and singled out one girl whose responses to the relevant questions were more pronounced than those of

the others. Intimidated by this unpleasant turn of events, the girl signed a full confession to the crimes, and the polygraph became indelibly marked in the annals of police history.

Though encouraged by this success, Larson remained skeptical. He differed from Marston (and most other polygraphers of the day) in that he did not believe there was any such thing as a characteristic "lie response." He was also enough of a scientist (he later became a forensic psychiatrist) to realize that the machine, as well as his own interpretations, could be plagued by a variety of errors. For that reason, he cautioned against ever using polygraph testimony as the sole source of evidence in a criminal trial. Larson was indeed ahead of his time, and it is unfortunate that most polygraphers today do not share his skeptical views.

John E. Reid

John E. Reid had a profound impact on the development of polygraph examinations, and today his is one of the biggest names in the commercial polygraph industry. He has his own company, John E. Reid and Associates, and the Reid College of Detection of Deception is named after him. He also coauthored the standard textbook for polygraph training and developed the idea of a "control" question and the control question technique (see Chapter 4).

In 1947, Reid published a paper in which he attacked the R/I test as being too imprecise. Reid (and others) had come to the conclusion that such questions as, "Did you murder John Smith last night?" or "Did you steal the five hundred dollars from petty cash?" were emotionally disturbing to the innocent and guilty alike. To counter these effects, Reid proposed a series of control questions to be interspersed throughout the test. These were designed to elicit strong responses from everybody and could be as simple as, "Have you

ever stolen anything in your life?"

Although simplistic in nature, control questions served the valuable purpose of getting people to lie for the record. Reid argued that everyone would be guilty of some minor transgressions of the law in their lives, but they would be afraid to admit to them during a polygraph exam because they would fear that it might affect their credibility or be the cause for some future action to be taken against them. Reid wanted to put this fear to use, so he made the assumption that most, if not all, individuals being tested would lie on these control questions. Their fearful responses to these questions could then be compared to their responses to the relevant questions. If a person is innocent of the crime under consideration, the theory goes, he or she will have a stronger pattern of responses to the control questions. If, on the other hand, the individual is guilty of the crime under consideration, he or she will show a stronger pattern of responses to the relevant questions.

The inclusion of this pseudocontrol has done more to enhance the credibility of the polygraph than any other "advance," but the technique is still flawed. As we shall see later, there are still serious questions about a polygraph exam's reliability and validity.

Reid's other contribution to polygraph examinations was the clinical lie test, which is structured around the concept of overt behavioral symptoms, or body language. One set of symptoms is supposed to be exhibited only when a suspect is being deceptive during an examination; another set of symptoms is indicative of how a nondeceptive suspect behaves. These behavioral symptoms have been exhaustively catalogued into two surprisingly long lists and form a branch of lie detection known as kinesiology, or applied kinesics.

Applied kinesics sounds impressive, but the idea that you can detect whether a person is lying based on

his or her body language is discredited by the vast majority of psychologists as well as by a good portion of today's practicing polygraphers. Don't, however, be lulled into a false sense of security—many polygraphers still use these lists as evidence that a person may be trying to be deceptive. Some of the behaviors that have been listed as indicating deception are: crossing your arms or legs, shuffling your feet, tapping your fingers, denying an accusation and immediately looking away, hesitating too long before denying an accusation, arriving late for the scheduled exam (this is a biggie and will weigh heavily against you), or leaving the examination room in a hurry once the examination is complete. All these responses are said to indicate deceptiveness, but any examiner who relies on this is opening himself up to a wave of criticism (and possibly even lawsuits) if he cannot prove the validity of these totally subjective interpretations. For example, I might think a three-second pause before answering a question is indicative of deception, but you might think seven seconds is necessary before we can really be sure that a suspect is lying. Who's right? Well, of course, neither of us is right because there are no overt behaviors that reliably signal deception. Unfortunately, a substantial number of polygraphers working today are basing their decisions on just this sort of evidence.

Cleve Backster

No history of the polygraph examination would be complete without mentioning Cleve Backster. Like Reid, he has his own school for training polygraphers, as well as a thriving commercial polygraph enterprise. Backster's approach, however, differs from Reid's on a major philosophical point: Reid's examiners are trained to use a "global" scoring technique that takes behavioral symptoms (kinesiology), "background," and other extraneous bits of information into consid-

eration, while Backster's examiners are trained to base their decisions entirely on the data contained in the polygraph charts. Backster is also credited with initiating a numerical scoring procedure for polygraph charts. This greatly increases the reliability of the polygraph exam because it allows similarly trained examiners to reach the same conclusions about an individual chart when that chart is scored independently. In other words, if you take ten Backster-trained examiners, put them in ten separate rooms, and give them ten copies of the same individual's chart, all ten should come up with about the same numerical score and, therefore, the same conclusion about that individual's deceptiveness or truthfulness.

The scoring innovations and reliance solely on the polygraph chart are certainly points in Backster's favor, but he has also conducted some research that many serious scientists consider laughably amateurish. In the 1970s, for example, Backster wondered what would happen if a plant was hooked up to the polygraph instrument. Now, obviously, a plant has no heartbeat, nor does it "breathe" in a way that could be readily picked up by the polygraph machine's rubber respiration tubes. A plant leaf does, however, have a relatively flat surface, so Backster attached the Galvanic Skin Response (GSR) leads from the machine to the surface of the leaf. Imagine his surprise when he observed polygraph tracings on the GSR channel that were similar to human responses! As the experiment progressed, Backster actually believed that the plant might somehow be reading his mind and responding. He would demonstrate this phenomenon by standing next to the plant and thinking about cutting off part of its stem. At times, the plant would "respond" with pronounced peaks on the polygraph chart—sort of a silent cry for mercy? Unfortunately, no one has been able to duplicate this feat, and it seems fairly likely that Backster's unique

responses had more to do with a poor experimental design or malfunctioning equipment than with some sort of psychic ability on the part of the plant.

LIE DETECTION TODAY

Diogenes probably never dreamed what a can of worms he was opening up when he roamed the streets of Athens with his lamp in search of an honest man. The search continues in earnest today, but the modern Diogenes gets paid for his services (some polygraphers make fifty thousand to sixty thousand dollars a year), and his "lamp" can cost upwards of five thousand dollars. Some other statistics that may surprise you about the current state of polygraphy in America are:

- * One million to four million private citizens submit to a polygraph exam each year.

- * 20 percent of the Fortune 500 companies and 25 percent of all other major companies use polygraph exams for screening purposes or for investigations into specific cases of theft.

- * Polygraph exams are most commonly used by banks, drug companies, department stores, fast-food emporiums, discount houses, and electronics firms.

- * Any business that has a large cash flow and high employee turnover is a prime prospect for a polygraph examiner.

- * Testing of federal government workers has tripled in the last ten years from seven thousand to twenty-three thousand.

- * Of the twenty-three thousand federal employees tested, 90 percent were being tested in criminal investigations.

- * The American Polygraph Association has about three thousand members, but there are an estimated ten thousand polygraph examiners practicing today.

- * Only half the states require polygraph examiners to be licensed.

- * A typical polygraph exam can cost from \$30 to \$150 a session, and some sessions take less than twenty minutes to complete.

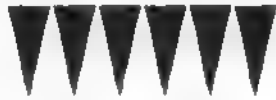
- * A polygraph machine can range in price from \$200 for a simple (GSR) recorder to \$5,000 for a full-blown five-channel continuous tracking "Diplomat" or "Fact Finder" machine.

- * One Atlanta, Georgia, company has cut costs to the bone by offering a most unique service: lie detection over the phone!

Indeed, polygraph examinations are big business. Some of you may be thinking, "Well, in a country of 250 million people, 4 million exams a year is really not that high a number." But you probably don't know any of the horror stories associated with them. In Chapter 2, you'll find out how ordinary, law-abiding citizens have been harassed, intimidated, coerced, and brutalized by "professional" examiners and why millions of innocent Americans are scared to death of polygraph examinations.

CHAPTER TWO

WHY BE CONCERNED ABOUT POLYGRAPH TESTS?



"Involuntary submission to a 'lie detector' test, upon pain of dismissal from employment, can constitute a tortious invasion of personal privacy, and . . . can amount to the intentional infliction of emotional distress, in contravention of the common law of North Carolina."

—Superior Court
of North Carolina
Restraining Order,
1979

Richard Nixon once said, "Listen, I don't know anything about polygraphs, and I don't know how accurate they are, but I know they'll scare the hell out of people." This fear is the greatest source of a polygrapher's power. An experienced examiner can easily manipulate a nervous and uninformed individual into believing just about anything.

What's worse, an experienced examiner can often extract personal and confidential information from an individual—information that would never be volunteered under different circumstances. The following set of questions, for example, were extracted from a lesson plan for the "Polygraph Examiner Training Course" taught at the U.S. Army Military Police School at Fort McClellan, Alabama. They train all federally employed polygraph examiners ex-

cept those in CIA. This lesson plan was used from February 1984 until November 1985, when it was discontinued because some of the questions were deemed unacceptable by the General Accounting Office.

What do you think about the following questions? More specifically, would you cooperate with the examiner if, during a "personnel screening," he asked you the following:

- * Do you have any friends who live in a foreign country?
- * Do you have any foreign pen pals?
- * Have you ever had a mental breakdown?
- * Have you ever been confined to a rest home?
- * Are you a name dropper?
- * Have you ever belonged to a hobby group?
- * While under the influence of alcohol, have you ever done anything you are ashamed of?
- * Have you ever owed a bar bill?
- * Have you ever assisted in the commission of an immoral act?
- * Do you desire to engage in unnatural sex acts?
- * Do you desire to continue engaging in unnatural sex acts?
- * Have you ever engaged in sex acts with animals?
- * Have you ever received sexual stimulation in a crowded area?
- * Do you receive sexual satisfaction through means other than bodily contact?

These questions are no longer used, but there are still plenty of reasons to fear a polygraph exam. A number of employers in the early 1980s stopped checking the references supplied on employment applications because they believed it took too much of their time and was just not worth the trouble. Instead, they turned to the polygraph exam because it was quick,

simple, and (for larger corporations) relatively cheap.

This practice was dealt a major blow in 1988, when Ronald Reagan signed the Polygraph Protection Act into law. There are now only a limited number of companies, plus the federal government, that can legally require polygraph exams as a condition of employment. This is not to say that the problems associated with using a polygraph for screening purposes have gone away—quite the contrary. There are still tens of thousands of hiring decisions made each year based on a series of scribblings obtained from a nameless, faceless machine.

Actually, it is not the machine that declares guilt or innocence, and that leads us to yet another problem: the woefully inadequate training given to polygraph examiners. I don't know about you, but I would rather not have my chances for employment controlled by someone who may have as little as six weeks of training (the average barber or hair stylist, by the way, must undergo nine months of training).

These criticisms are minor, however, compared to the charges of ineptitude and lack of professionalism that have been leveled against some polygraphers. If you think that you have nothing to worry about by taking a polygraph exam because you have never done anything criminal in nature, then you are sadly mistaken. Many of the people you are about to meet also believed they had nothing to fear because they were innocent. They quickly realized that "innocence" can be a relative term, and anyone, no matter how honest, can one day become a victim of false charges or unsubstantiated accusations dealt out by an overzealous polygraph examiner.

INNOCENT UNTIL PROVEN GUILTY?

John Tillson was a civilian budget analyst working for the U.S. Department of Defense (DOD). Because of

his position, he was present at a variety of upper-level DOD meetings during which budget proposals were formulated and discussed. In January 1982, he attended a meeting that would change his life forever.

It all began with a fairly typical meeting of the Defense Resources Board (DRB). The board, composed of several assistant secretaries of defense as well as senior Pentagon officials, met to discuss President Reagan's defense budget. As the meeting progressed, the board soon realized that Reagan's proposed arms spending plans would exceed the defense department's budget by a whopping seven hundred billion dollars.

Understandably, the DOD did not want this explosive information to reach an already distrustful and economically jaded American public. Unfortunately, it did. The *Washington Post* somehow obtained this information from one of the participants at the DRB meeting and ran the story on the front page. Senior DOD officials were outraged and ordered polygraph examinations for everyone who had attended that meeting, including the joint chiefs-of-staff and then Deputy Secretary of Defense Frank Carlucci. Everyone at the meeting passed the lie detector tests except one man—John Tillson. A second polygraph test was given, and then a third, but Tillson failed all three times. Convinced that they had found the source of the leak, the DOD was ready to take action. Tillson, understandably shaken, pleaded his innocence. He was a West Point graduate and a Vietnam veteran, and he swore that he had not told anything to anyone after the DRB meeting had adjourned. The most he would admit to, after exhaustive interrogation, was the possibility that he had spoken with some unauthorized individuals *before* the meeting took place, but he steadfastly denied talking to anyone after the meeting.

Pentagon officials remained unconvinced until they received a letter from the *Post* reporter clearing Tillson.

Although the reporter would not reveal the true source, he did confirm that Tillson was in no way involved. Due to a lack of any other substantial evidence against Tillson, the DOD grudgingly decided not to fire him.

HOW CONTROL QUESTIONS CAN WORK AGAINST YOU

Control questions can mean different things to different people. Polygraph examiners generally assume that everyone lies on control questions because we have all committed some minor indiscretion during our lives. The theory is that innocent people will show greater emotional reactions to these questions than to questions that are directly relevant to the crime under investigation. Unfortunately, it doesn't always work that way, as the following two cases point out.

In one instance, a small-town bank discovered that four thousand dollars was missing from the vault. All the bank's employees were summarily tested, including a woman with twenty years seniority who had never been accused of anything like this in her life.

As the equipment was strapped on, she could feel her anxiety level rising. When they asked her "Did you take the four thousand dollars," her anxiety peaked—she experienced a momentary disruption of her respiration, and her heart pounded in her chest. The control questions also resulted in elevated responses, but none were so extreme as those associated with the relevant questions having to do with the actual theft. Unfortunately for her, "innocent" individuals are not supposed to react this way, and she was fired on the spot. She had not taken the money, but a polygraph examiner assumed that she had, simply because she did not respond as strongly to the control questions as she had to the relevant questions.

In another case, a woman was raped in her apart-

ment by an unknown intruder. Not only did the intruder penetrate his victim vaginally and orally, but, among other perversities, he shaved off her pubic hair. She reported all of this to the police, and instead of comforting her, they further prolonged her ordeal. Apparently, the local sheriff had "read somewhere" that shaving off the pubic hair was a telltale sign of a lesbian rape. He asked the woman to submit to a polygraph examination so that they might determine whether the assailant was male or female. Although the woman was outraged over the assumption that the rapist might be a woman, she reluctantly submitted to the exam. Failure to do so, she reasoned, would impede the investigation because the sheriff would continue to believe that the attacker was a woman. Despite her misgivings about polygraph exams in general, the woman believed that the examiner would have to confirm her contention that the rapist was male. How could he possibly find otherwise? As you may have already guessed, this confirmation would not be forthcoming.

A problem arose when the Backster-trained examiner used, "Between the ages of eighteen and twenty-five, did you ever have sex with a woman?" as a control question. Apparently, this examiner had also "read somewhere" that every thirtyish divorcée living alone with her ten-year-old child has had at least one homosexual experience after the age of eighteen. When the woman answered "no" to this question, the examiner had to assume that this was a lie because of the way the test works. And because her responses to this control question were lower than the responses elicited from the relevant questions, the examiner had to assume that the woman was lying about the intruder being a man. Despite her protests, this was the "expert opinion" he put forth in his final report. The male rapist, consequently, had ample time to lose

himself while the police department was busily searching for a lesbian rapist.

CAN A MACHINE BE FOOLED?

This is a case with an ironic twist. Usually, private citizens are the ones who suffer at the hands of police officers or other polygraph "experts." However, John K. is a deputy sheriff in Minnesota, and he had a crafty prison inmate turn the tables on him.

It all began when the inmate retrieved a hunting knife and loaded gun from his cell and gave them to a visiting federal marshal. The inmate explained that he had bribed a guard to smuggle the weapons in so that he could escape, but that he had since had a change of heart and no longer wanted to make the attempt. The federal marshal believed the inmate's story and asked which guard had supplied him with the weapons. Without batting an eye, the inmate replied that John K. had smuggled in the weapons.

This accusation resulted in polygraph examinations for both the inmate and John K. The inmate passed with flying colors; John K. flunked. Had John K. really smuggled weapons to an inmate? The Minnesota Bureau of Criminal Apprehension (they administered the polygraph) was satisfied that he had.

John's commanding officer (a sheriff) was skeptical, however, because of a letter he had received recently from a local merchant, praising John's actions. The letter told how John had gone to this merchant to buy a gift for his son, when through some sort of mix-up, the present was put in a bag containing the store's receipts, charge slips, and several hundred dollars in cash. John noticed the error when he got home, and he called the merchant immediately to tell him that the store's money was safe and would be returned when he drove to work the next morning. The sheriff realized that this

story and the charges currently leveled against his deputy did not match up. Why would a man accept bribes one day and return several hundred dollars in cash the next? He began to look for other possibilities, and his thoughts turned to the inmate.

Could the inmate have lied? And if so, what had been his motive? The answer became clear when the inmate escaped from a less secure facility. Apparently, the inmate had carried out the entire ruse so that he would be transferred to a much less secure institution. This ingenious plan was verified by the inmate shortly after his recapture, when he told investigators that John K. had merely been an unwitting player in the grand scheme. In other words, the sheriff had been right, and the Minnesota Bureau of Criminal Apprehension had been wrong; the inmate had lied during his polygraph exam and been labeled truthful, and John had told the truth during his exam and had been labeled deceptive.

Do you still think you have nothing to be afraid of?

FACT: In Ohio, a man accused of murder flunked two polygraph exams given by different examiners. After being tried, convicted, and sentenced, other individuals confessed to the crime.

FACT: A North Carolina man accused of murdering his wife failed a polygraph exam, and the police were ready to file formal charges against him when she returned home from an unannounced trip.

FACT: In California, a supermarket cashier was accused of giving her mother unauthorized discounts. A polygraph exam confirmed the store's allegations, but the cashier had an airtight alibi: her mother had been dead for five years. Apparently, a combination of shock and grief had colored the girl's responses.

These examples show how things can go wrong even when polygraphers follow all the rules. More disturbing, however, are those cases in which police or

unscrupulous private examiners coerce, threaten, and intimidate innocent individuals.

POLICE INTIMIDATION AND OTHER ABUSES

David Lykken, probably the most outspoken critic of polygraph examinations, has said that the Peter Reily case should be read by every polygrapher, prosecutor, and juror in cases where repudiated confessions figure into the evidence. You may already know about this case from the best-selling 1976 book, *A Death in Canaan*, by Joan Barthel (a movie has also been made).

The facts are as follows. Eighteen-year-old Peter Reily returned home late one evening to find the grossly mutilated body of his mother. The police were notified immediately and, upon arriving at the house, ushered Reily to the backseat of a patrol car. There, he waited for three hours while police conducted their preliminary investigation. What Peter didn't know was that the police were already forming strong suspicions about him—suspicions they hoped to confirm through a polygraph examination.

Early the next morning, Peter, having had only two or three hours of sleep the night before, consented and was hooked up to a polygraph instrument. Not surprisingly, he reacted strongly to questions such as, "Did you hurt your mother last night?" (I think most of us would react strongly to questions about our parents if we had found their mutilated bodies less than eighteen hours ago!) Although the young man initially denied all the police's allegations, the lack of sleep and general state of shock began to take its toll. He became confused and frightened and slowly began to tell the police examiners what he thought they wanted to hear.

Because the several-hour examination was tape recorded, psychologists have since been able to study

how a skilled examiner can "affect an attitudinal shift" (i.e., brainwash) to a "subject of diminished capacity" (i.e., a tired and confused kid). A variety of exchanges between Peter and the examiners went something like this:

Peter: I couldn't have done anything like that last night. I just couldn't. Maybe your machine is wrong.

Police: No, Peter. The machine's not wrong because it's just a recording of your mind. You understand? These charts just tell us what's going on inside you.

Peter: Well I don't understand it. I'm sure I couldn't have done it. I don't remember it. If I had done it, I'd tell you. I'm not purposely trying to deny anything. I just don't remember . . . I don't know.

Later, as the interrogation got more aggressive, the ordeal began to take more of a toll on Peter. The following types of exchanges occurred:

Police: Look, Peter, we just want to get at the truth. We just want you to tell us what you did last night. Did you hit her? Did you kick her?

Peter: I don't know. I could have. You say I kicked her, and I can see myself doing it . . . imagining it.

Police: No, Peter, you're not imagining anything. It's the truth, and it's just trying to work its way out. You know, we know that this is hard for you, but you gotta try. You've gotta let the truth come out. Don't fight it.

Peter: Well, maybe. Maybe I'm just having a hard time accepting it myself. I'm just not sure . . .

Later on in the interrogation, Peter finally broke down and told the police, "Well, it really looks like I did it." Naturally, while all this was going on, the real murderer was covering his tracks and trying to put as much distance between himself and the Reilys' Connecticut home as he could. Two years passed before Peter's confession was finally proven false, and the police were left with a bizarre crime, no suspects,

and red faces for having relied so heavily on their coerced polygraph "evidence."

The police don't always wait for murder cases to roll around to use their magical machine, but an unsolved death can often start the gears turning in a polygrapher's head. A Georgia murder, for example, had the police stumped. There were few clues and even fewer suspects. As public pressure mounted, the police arrested a young black kid and proceeded to harass and intimidate him. They eventually strapped him to a polygraph machine and told him that the machine could tell if he was lying or telling the truth, and that if he was lying, that the machine would electrocute him!

Now you and I may laugh at such an obvious trick, but remember that this was a poor, uneducated kid who had never been more than ten miles away from his home in rural south Georgia. Quite simply, he panicked. He really thought that the polygraph machine would electrocute him, so he admitted to everything that the police asked him about. And what was the result of this sham? Suffice it to say that prosecutors, judges, and juries don't put much faith in blatantly coerced confessions. The kid was released, and the police were back to square one.

Then there is the case of the police in Radnor, Pennsylvania, who wanted to get a quick confession out of a suspect they had just apprehended. Instead of using a real polygraph machine, however, they decided to make one of their own. One cop got a metal colander (like you would use to drain spaghetti) and attached a couple of pieces of wire to it. They ran these wires to the back of a Xerox machine and taped them in place. Finally, they typed "HE'S LYING" on a piece of paper and placed it in the machine so that it could be copied repeatedly. With their "polygraph machine" ready to go, police sat the suspect down, put the colander on his head, and began their interrogation. Whenever they

received an answer they didn't care for, one of the cops would hit the "copy" button, and out would pop the message "HE'S LYING." Convinced that the machine could read his mind, the suspect confessed.

A variation of this trick has been used by police officers in several states. When they believe they have apprehended a naive suspect, the officers will wrap the squad car's microphone cable around the suspect's arm and begin the "interrogation." Unwanted answers are easily contradicted by one of the officers surreptitiously pressing the TRANSMIT button on the microphone. Pressing this button activates a red light on the car's radio, and the officer will say, "See there? See that red light? That says you're lying. You're not lying to me are you? Let's try it again." This little scenario will continue either until the suspect confesses or the officer thinks he's not getting anywhere.

SOME ALARMING STATISTICS

So you see, you don't even need a real polygraph machine to force a confession out of a suspect. These case studies should have convinced you that polygraph exams and examiners are fallible, and that you should approach these exams with a great deal of caution. But if none of this has convinced you yet, perhaps this sobering statistic will: it has been estimated that 40 to 50 percent of truthful individuals have been misdiagnosed by examiners. In other words, if you are a suspect in a criminal investigation, you have a one-in-two chance of being labeled "deceptive," even if you have no knowledge whatsoever of the crime. What's more, the Office of Technology Assessment (OTA), an arm of the federal government that analyzes and evaluates current technology, reviewed more than four thousand bibliographic entries concerning polygraph exams and found that only thirty-five to forty met any

of the basic scientific criteria for a properly controlled research experiment. And of these forty or so articles, OTA found that the polygraph's ability to detect lies was as low as 50.6 percent (I can *guess* and be right 50 percent of the time!), and its ability to detect the truth ranged from a high of 94.1 percent to a dismal low of 12.5 percent.

These figures should shock you because thousands of these exams are given in the United States every working day. The polygraph industry rakes in millions of dollars every year—largely at the expense of decent, law-abiding citizens. Of course, if the polygraph machine really worked, there wouldn't be any need for me to write this book or for you to read it.

Polygraphers will tell you that their machine is correct 90 to 95 percent of the time, but let's look at what that really means. Imagine a situation in which 1,000 suspects are rounded up, but only 50 of them are actually guilty of a crime (which they all deny). If we assume that the polygraph validity rate is 90 percent for both guilty and innocent individuals, then 45 members of the guilty group will be correctly identified, and five will beat the test. Of the 950 innocent suspects, however, 95 will be misidentified as guilty! Remember, too, that these figures all assume that polygraphers are right 90 percent of the time. Imagine how many more innocent people are misclassified as a polygrapher's "correct" rate drops to 80, 70, or even 50 percent!

No matter what they tell you, polygraph examiners cannot be correct 100 percent of the time. They cannot always be correct because they are human, and humans make mistakes. But should the innocent suffer because the polygrapher didn't get a good night's sleep or because his child is at home in bed with the flu? For that matter, should an innocent individual be misidentified because he (or she) had a bad night's sleep or has a sick child?

BEATING THE BOX

Is there anything we can do to protect ourselves? You bet there is! Thousands of people have learned how to beat the box, and so can you. It's really not very hard; it just takes a little concentration and practice.

A man by the name of Floyd Fay, who was wrongly convicted of murder based on a polygraph exam spent two years behind bars before he was cleared. In that time, he became an expert in beating polygraph exams. In fact, he got so good at it that he taught other inmates his techniques. (Inmates are given polygraph exams often concerning violations of prison rules. Knowing how to beat a test can mean the difference between staying at one facility and being transferred to a maximum-security prison with the really hard-core offenders.) By his account, Fay coached twenty-seven inmates scheduled to take polygraph exams; all freely admitted to him that they were indeed guilty of the charges (which were usually drug related). After about twenty minutes of instruction, twenty-three of the twenty-seven managed to beat the test, which equates to a very respectable 85 percent success rate!

The rest of this book is dedicated to the practical aspects of the polygraph: what it is, how it works, and how you can beat it. Even if you remember only a little bit of the information herein, you will still be better prepared should you ever find yourself the unfortunate target of a criminal investigation, and you will have much less reason to fear a "preemployment screening" or an "aperiodic honesty check." If you read carefully, practice, and keep your wits about you, then in no time at all, you should have the skills necessary to beat the box!

CHAPTER THREE

THE INSTRUMENT AND THE EXAMINER



"On a more pragmatic level, the lie detector does work as long as the subject believes it works. A good examiner scares the crap out of you. It's theater."

—Leonard Saxe,
principal author of
the OTA's
1983 polygraph
validity study

Up to this point, I have told you to be both cautious and skeptical of the polygraph machine. In all fairness, however, you don't really have to be afraid of the machine—only the operator. You see, the machine itself is a very reliable instrument that can accurately measure and record your respiration, perspiration, pulse, and skin conductance (for five thousand dollars, it ought to be able to do something well). In fact, no one I know of has ever criticized the actual machine unless the pen plotter ran out of ink or the chart-drive jammed.

Criticisms abound, however, when one person uses these innocuous physiological tracings to infer that another person is lying. In other words, the fault lies solely with the polygraph examiner, not the polygraph machine. This is important to remember if you are

taking a polygraph exam and a polygrapher says, "No, the machine doesn't make mistakes. It can't lie." You should quickly remind yourself that it's not the machine you are worried about—it's the examiner. Let's take a look at the machine and its operator.

THE POLYGRAPH MACHINE: WHAT IT IS AND HOW IT WORKS

People are often impressed with or intimidated by the polygraph machine when they first see it because it is such a complicated-looking piece of electronic hardware. By comparison, my VCR is also a pretty complicated-looking piece of electronic hardware, but I don't know anyone who is overly impressed with it or threatened by it.

Is this a fair comparison? Probably not, because people see VCRs every day in their homes, in magazine advertisements, in department stores, and in television commercials. Most people, however, will see a polygraph machine only once—on a small table next to a hard chair in a sparsely furnished room. Remember, too, that VCRs and polygraph machines will most likely be encountered under vastly different circumstances. Most people would not be afraid to go to a shopping mall if they knew VCRs were sold there. Most people are very anxious, however, if they know that they have to go to a downtown office building or hotel room to take part in a polygraph examination. In other words, going to a shopping mall is not normally an anxiety-arousing experience; going to a polygraph exam is.

But you no longer have to be afraid of the machine! They are not much more complicated than a VCR, and there is not any great amount of variation from model to model.

Most polygraph machines in use today are portable and are about the size and shape of a standard briefcase.

On one side of the machine is an approximately eight-inch-wide (this varies with respect to the manufacturer) ribbon of paper on which your responses are recorded. When the test begins, this paper will travel across the top of the machine (under a series of pens) and exit through a side opening. This gives the examiner easy access to your plotted responses during the exam, and it gives him a hard copy of your responses for future examination or reference. This component of the machine is called the *chart drive*.

Suspended above the chart are anywhere from three to five or more pens that fluctuate with respect to your level of arousal. This is called the *pen plotter*, and it may differ from machine to machine, depending on how many *channels* are being recorded. A three-channel machine, for example, will usually record heart rate, skin conductance, and rate of breathing. A four-channel machine does the same thing, but it may take two separate recordings of respiration. This is done through *pneumographs* that are strapped around the body. A pneumograph is nothing more than a rubber tube that expands and contracts as you breathe. These tubes are placed around the chest (three-channel machine) or around the chest and abdomen (four-channel machine) in order to accurately gauge any irregularities in your breathing patterns. Cardiovascular activity (heart rate or blood pressure or both) is recorded with a *sphygmomanometer* (blood pressure cuff) placed around the biceps. Skin conductance is measured by placing *electrodes* on the fingertips. These are generally held in place with Velcro, and the examiner may or may not apply some sort of conducting jelly to the fingertips before they are attached.

The pneumographs, blood pressure cuff, and electrodes are all wired to the machine so that your responses can be fed to the pen plotter. Most machines will electronically enhance one or more of these leads

before they reach the pen plotter. The blood pressure reading is enhanced, for example, so that the cuff does not have to be fully inflated, which would restrict blood flow to your lower arm and hand. Skin conductance may also be enhanced so that the peaks and valleys recorded on the chart are more pronounced and easier to read. Some have said that this enhancement alters the pen plotter's tracings and, therefore, should not be used. This is really an unfair charge because the electronic enhancement is not altering the patterns or tracings, it is merely amplifying them. Think of it this way: if you can't hear the quieter sections of a cassette tape you are playing, you just turn up the volume. You haven't altered the music, you have just made it easier to hear. The polygraph machine works the same way. It "turns up the volume" on your physiological reactions so they are easier to read and interpret.

Consider, though, that if you turn up the volume on a bad cassette, you still have a bad cassette, only louder. Likewise, you can enhance a person's physiological measurements all you want, but it won't make you any more accurate in formulating an assessment of that person's veracity. No amount of electronic gadgetry will have an appreciable effect on polygraph validity because the polygraph exam itself is an inherently bad system based on a variety of bad techniques.

THE POLYGRAPH EXAMINER: WHO HE IS AND HOW HE WORKS

Does a career involving a minimum amount of education beyond a high school diploma (six weeks of training and a nine-month apprenticeship) that can lead to a fifty- to sixty-thousand-dollar-a-year career sound too good to be true? Well, it's not. All you have to do is run down to your nearest polygraph training school and

sign up for "a challenging and rewarding career in the fast-paced world of lie detection!"

Despite what you might think, not all polygraphers are former police officers, military men, private detectives, or CIA agents. Many are just your average high school graduates, college dropouts, or college graduates who realized they could make a lot more money as polygraph examiners than as assistant managers at the local fast-food joint.

In one respect, these types of examiners may treat their examinees more fairly, because they don't have the preconceived notions that seem to be inherent in a lot of former cops, for instance. One examiner who had been a police officer was captured on a hidden camera saying that he could usually tell within five minutes of meeting a suspect whether or not that suspect was guilty. This is the ultimate in polygrapher arrogance. If the examiner can really make that distinction almost immediately after meeting someone, why does he need the machine? I suspect that police officers are more prone to make this type of error than "civilians," because they have encountered the criminal element on an almost daily basis.

This is not to say that civilian polygraphers do not make determinations of guilt before the test has even been run—they do. In fact, I don't know of anyone who can meet an individual for the first time and not form some sort of opinion about that person. It's human nature. This is precisely why no polygrapher can be completely objective as he scores and interprets the charts. His personal biases and opinions are incorporated automatically (consciously or unconsciously) into his decisions, whether or not he recognizes it. He may say his decisions are totally objective, but how do we know he doesn't harbor some personal dislike toward men with long hair, Mexican-Americans, divorced women, Catholics, or any of a

hundred other demographic characteristics? The fact is, we don't know, and we can't tell unless we ask him, point blank, whether or not he is biased against a particular group of people. And even if he tells us he's not, how do we know he's not lying? Maybe we could strap a polygraph machine on him and give him a taste of his own medicine . . .

Civilian Training

It is difficult to talk about civilian polygraph training because there are so many theories and techniques taught at so many independent schools. But one major disagreement exists between the competing Reid and Backster organizations.

The Reid school trains its students to use what is known as global scoring. This entails: A) reading the suspect's case file and other supplemental materials, B) conducting the pretest interview, C) formulating the test questions, D) administering the test, E) conducting the post-test interview, F) considering all the behavioral patterns exhibited by the suspect during steps B through E, G) evaluating the polygraph charts, and H) reaching a final determination of deceptiveness or nondeceptiveness. The Reid school also teaches that special attention should be given to the behavioral patterns emitted by the suspect because it is the examiner who actually detects lies. The machine may provide the charts, but it is the examiner's training, insightfulness, and experience that create an overall impression.

The Backster school, on the other hand, deemphasizes global scoring in favor of straight chart interpretations. Teachers at the Backster school will not have students memorize long lists of "deceptive" behaviors, nor will they tell them to give their subjective impressions more weight than the actual charts. At a Backster school, students will learn how to score a chart numerically and base decisions

entirely on the data provided by the charts.

If I were ever suspected of a crime and chose to submit to a polygraph exam, I would much rather have a Backster-trained examiner administer it for two reasons: 1) I would know that he was using the most objective methods available to score my charts, and 2) I would not have to worry about whether or not I arrived late for the session, how I was dressed, or whether I sat with my legs crossed or not. Reid examiners will take all of these factors into consideration; properly trained Backster examiners will not.

Of course, another problem is that not all polygraph examiners are taught at either of those schools. At least with Reid- and Backster-trained examiners, you have some idea what they are looking for and how your exam will be scored. The hundreds of other independent schools (which, by the way, usually need no state licensing) and police forces may teach totally different techniques. I can easily envision a school that uses some of Reid's ideas, some of Backster's ideas, and some ideas that a staff member happened to pick up in an introductory psychology course taught at the local community college. Some schools might emphasize the GSR channel, others might emphasize changes in blood pressure.

This lack of standardization can only hurt the polygraph industry in the long run as more and more unaccredited schools turn out more and more unqualified examiners. Furthermore, there is no real "continuing education" in the polygraph industry. The implied message is that once you have graduated, you know all you need to know for the rest of your life.

There are journals that publish pro polygraph articles almost exclusively (*Journal of Polygraph Studies*, *Polygraph*, *Journal of Polygraph Science*), but most of those articles should be taken with a grain of salt. The *Journal of Polygraph Science*, for example,

recently ran a piece entitled, "Clothes Make the Polygraphist."

What is the overall evaluation of civilian polygraph training? Like many things in life, some is good, some is bad, and some is so substandard that it is a real dilemma for the truly committed professionals who are trying to raise the polygraph industry above the realm of technological mysticism. The most important step the civilian polygraph industry can take is to adopt some sort of standardization for tests so that all polygraphers adhere to at least some basic methodology. As it stands now, polygraph results are a lot like psychiatric opinions of insanity: there will never be a consensus. If you've been judged deceptive three times, keep looking and you'll almost certainly be able to find three examiners who will vouch for your truthfulness.

Military Training

Unlike civilian polygraph training, the military has only one school that teaches FBI, Secret Service, National Security Agency, and military investigators. This polygraph brain trust is located in Building 3165 at Fort McClellan, Alabama, home of the U.S. Army Military Police School (USAMPS). The polygraph is taken very seriously there, a fact fresh recruits learn quickly. Anyone uttering taboo words such as "Ouija Board," "hot question," "squiggly lines," "innocent," "guilty," "thingamabob," or "lie detector" is forced to make a contribution to the class fund. Upon graduation, the accumulated money goes toward a graduation picnic.

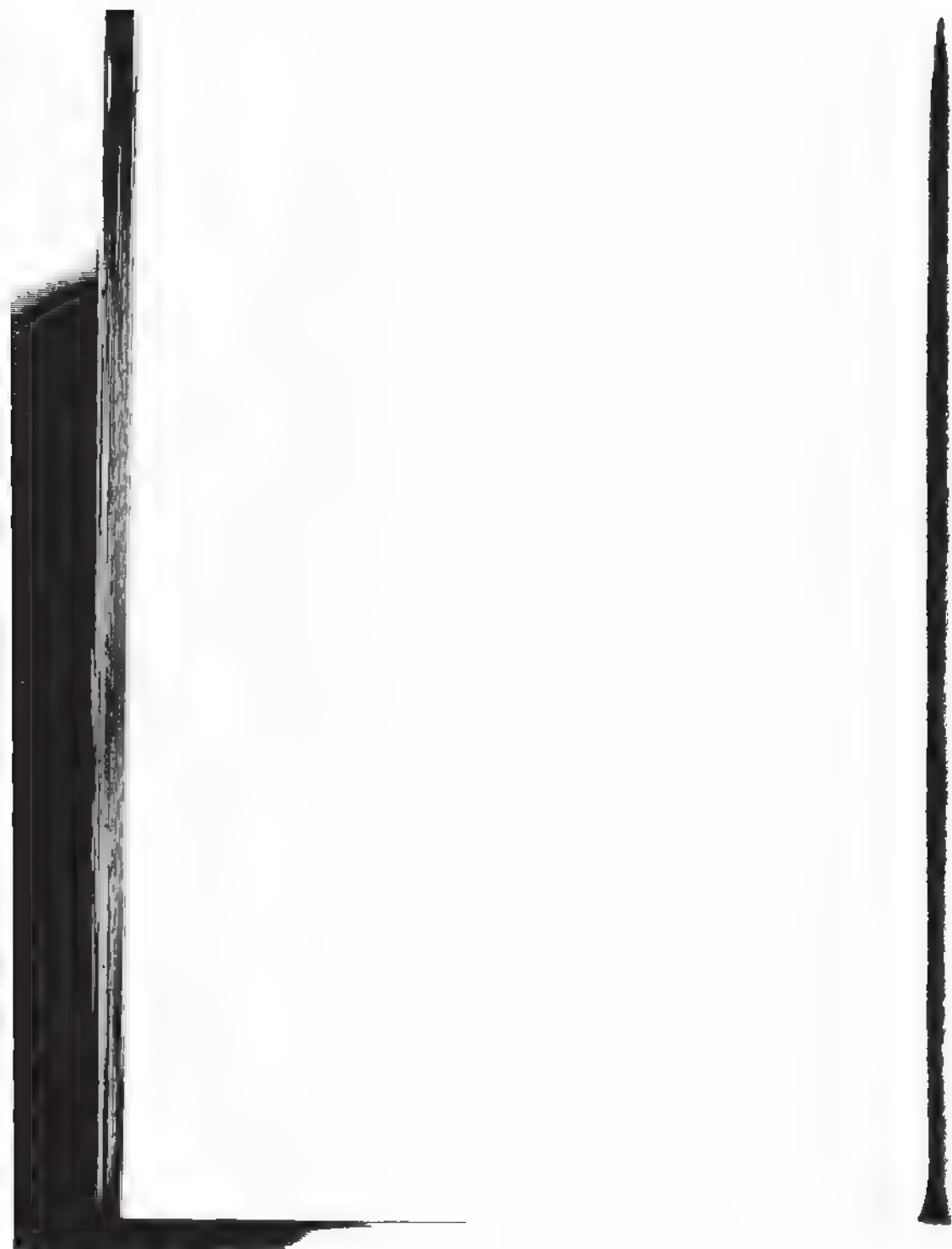
Not surprisingly, the training at Fort McClellan's polygraph school is militaristic and rigorously structured. Instead of the typical six-week course administered by civilian schools, Fort McClellan trains for fourteen weeks. Weeks one through four include lectures on law, semantics, ethics, physiology, psy-

chology, pharmacology, testing procedures, and machine operation and maintenance. Weeks five through fourteen are devoted to practice sessions so that the student can apply what he is supposed to have learned.

The results of this strict training are evident: Fort McClellan is widely acclaimed as the best polygraph training facility in the world. In fact, the world often comes to Fort McClellan in the form of foreign government agents: Taiwan, Israel, Venezuela, and South Korea have all sent agents to the infamous Building 3165 for training. There is no doubt that polygraph examiners trained at Fort McClellan are better prepared than the majority of civilian examiners.

Should you be concerned, then, if you ever find yourself across the table from a McClellan graduate? I don't think so. As long as you can control your emotions and remain calm, you should never have to fear any polygraph examiner—no matter how qualified he is. Remember, Fort McClellan may turn out the best polygraphers in the world, but the underlying theory of what they teach is still flawed. No amount of training can compensate for the fact that there are no reliable physiological responses correlated with telling a lie. Of course, polygraph examiners will never admit to this. They will instead try to overtly or covertly coerce you into believing you are helpless against their advanced technology and knowledge.

Don't believe a word of it! If they were as good as they say they are, then we would have no more need for judges or juries or any other part of the judicial system. A polygrapher could just test suspect after suspect until he found a guilty one, and then throw him in jail. This hasn't happened yet, nor is it likely to—especially since the machine is so easy to beat in the first place.



CHAPTER FOUR

THE TESTS



*"The whole process
smacks of twentieth
century witchcraft."*

—Sen. Sam J. Ervin

If you should ever do some additional reading in the field of polygraphy, you will come across a number of phrases that are synonyms for "polygraph test." Among these are "polygraph exam," "polygraph screening," "polygraph evaluation," "polygraph interrogation," and, occasionally, "deceptograph." While these are all useful synonyms, it should be noted that most of them are technically inadequate.

WHEN IS A TEST NOT A TEST?

The American Psychological Association (APA) is very exacting when it comes to terminology. Do you see a significant difference between the words "test," "screening," and "interrogation"? The APA certainly does. Only the phrase "psychological test" has a clear-cut, standardized definition.

To be properly labeled a psychological test, an examination must meet four basic criteria: standardized method of administration, immediate recording of behavior, objective scoring, and external validity. Using these criteria, can we properly call a polygraph exam a psychological test? Let's find out.

Standardized method of administration. The number of training schools and varying techniques violates this rule.

Immediate recording of behavior. The polygraph does immediately record the rate of perspiration, respiration, and heartbeat, but if the examiner is using a global scoring technique, then "overt psychomotor behaviors" may not be recorded for minutes or even hours after the formal examination has concluded.

Objective scoring. Only a small subset of today's polygraph exams are scored objectively. The vast majority of determinations are made by combining chart data with the examiner's subjective impressions of the subject's personality.

External validity. There are no data demonstrating the validity of an examiner's subjective appraisal of veracity.

Judging from these criteria, it appears that a polygraph "test" is really not a test at all. But if it's not a test, then what should we call it? Perhaps the word that best describes the whole polygraph procedure is "interrogation." The accused is not being tested per se; he/she is merely taking part in a data-gathering session. The polygrapher's job is to pick out the relevant from the irrelevant. Unfortunately, whenever a polygrapher compares and combines objective polygraph data with subjective clinical assumptions, all of the criteria for a valid psychological test are violated. Consequently, polygraph tests, for the most part, are best described as interrogations. Realize that when I refer to them as "polygraph tests," it is merely for the sake of brevity.

TYPES OF POLYGRAPH TEST QUESTIONS

Almost all polygraph exams are composed of three types of questions: relevant, irrelevant, and control. The primary difference has to do with the frequency and placement of each of these types of questions. Some examiners, however, will administer an exam that contains only one type of question, the guilty knowledge question, which is used to determine whether you know certain facts about a crime that you couldn't possibly know unless you were the guilty party. As we examine all four of these types of questions, pay careful attention to the characteristics of each; you will need to be able to identify the type of question being asked in order to defeat a polygraph exam. At the end of this section are some sample tests, which I encourage you to run through a number of times in order to get the feel of how a polygraph exam works and to test your knowledge. Remember, polygraph examiners rely on the assumption that they know more about how an exam works than you do. Don't allow them this advantage over you. Knowledge is power! The more you know about polygraph examinations, the better off you will be.

Relevant Questions

Relevant questions are those which are directly related to the focus of an investigation. As such, a relevant question can be very narrow and specific ("Did you steal the three hundred dollars from the cash register on the evening of July 23?") or, when the area of interest may be an individual's entire background, very broad ("Have you ever been disciplined on the job for alcohol or drug abuse?"). Relevant questions are usually easy to spot because they will almost always relate to whatever incident (or crime) is under investigation. One exception to this rule involves

interrogations conducted by intelligence agencies. Should you ever find yourself under examination by an intelligence agent, you should prepare yourself for questions concerning unauthorized contact with foreign intelligence agents or involvement in Communist activities. Questions in an intelligence screening might also deal with aspects of an individual's life that would make him/her susceptible to blackmail. It is important to note, however, that when several relevant questions must cover a variety of equally important issues (e.g., political leanings, criminal record, and so on), the individual under examination is not expected to exhibit elevated physiological responses to all of them, and the relevant questions that do not evoke higher-than-normal responses are used later as control questions.

This brings up an important point about the relationship between relevant, irrelevant, and control questions. They can switch from one category to another depending on the specific context in which they are used. Consequently, any questions presented here as an example of a particular category may change categories under different circumstances or even at different times during the same interview.

Suppose the retail store where you work has been experiencing a lot of lost (and presumably stolen) inventory. You have voluntarily submitted to a polygraph exam, and you are asked the following question: "Have you ever consumed alcoholic beverages during working hours?" Is this a relevant question? In this instance, it is not. It is a control question designed to make you feel anxious about the consequences of being caught drinking on the job. And since many employees will have the occasional beer at lunch or glass of wine at an office party, it does work well to raise doubts in your mind and make you unusually anxious.

Now consider a different situation. You are a delivery driver for an antiques store. One Friday afternoon, you crash the truck into a tree and leave the scene of the accident. Later that evening, you phone your employer and tell him you "blacked out" while driving and don't really know what happened. Suspicious, your employer asks you to take a polygraph exam in order to prove your innocence. You agree, and the examiner asks you the following: "Have you ever consumed alcoholic beverages during working hours?" In this instance, this is a relevant question, because drinking could very well be a cause of the accident and is therefore relevant to the issue under investigation.

Irrelevant Questions

Irrelevant questions, while seemingly innocuous, serve a very important purpose in that they allow an examiner to chart an individual's normal, baseline level of arousal. A comparison can then be made between baseline arousal and arousal brought about by the relevant questions. In order to maximize the difference between response levels, irrelevant questions are designed to have very little emotional impact on an individual. A typical irrelevant questions would be, "Is today Friday?" or "Are we in the state of Florida?" Of course, irrelevant questions may become relevant, depending on an individual's response. So, for example, if you show unusually strong emotion to the question, "Is your name John Smith," the examiner may suspect that you are hiding behind a false identity and decide to treat that question as a relevant one instead.

Control Questions

Like irrelevant questions, control questions are used for comparison with relevant questions. The critical difference is that control questions are not used to establish a baseline, but to elicit a strong emotional

response. In order to effectively defeat a polygraph exam, you must be able to recognize any control questions that may come your way. One type concerns what is considered to be related indirectly to the issue under investigation. For example, in a criminal investigation involving the theft of money from a desk drawer, a control question might be, "Have you ever stolen anything of value in your life?" For an insider trading probe, a control question might be, "Have you ever betrayed a confidence?" Again, control questions and relevant questions are easily interchangeable, depending on the circumstances. This has led to controversy among polygraphers over the use of so-called "inclusive" versus "exclusive" controls. Inclusive controls probe the incident under investigation indirectly. For example, an incident involving the theft of three hundred dollars from a cash register could produce the following:

Q. Have you ever stolen money from an employer?
(Inclusive control.)

Q. Did you remove the three hundred dollars from the cash register? (Relevant.)

Exclusive controls, on the other hand, cover a period of time exclusive of the incident under investigation. So continuing with the cash register example, we get:

Q. Before the age of eighteen, did you ever take anything of value? (Exclusive control.)

The controversy surrounding inclusive versus exclusive controls involves the concept of "psychological separation." Some polygraphers argue that suspects under investigation treat inclusive controls like relevant questions (i.e., they do not treat them as separate, independent categories). This "lumping together" of the controls with the relevants would

defeat the purpose of the control question and thus invalidate the test. This is the position taken by the federal government, so you should never encounter inclusive control questions during a government interrogation. Private polygraph firms, however, will often use both inclusive and exclusive controls.

Concealed Information Questions

The use of concealed information questions is based on the assumption that the guilty individual will know (and remember) specific details of a crime that no innocent person could possibly know. Such information might include details about the site of the crime or the means of committing it, such as the technique used to enter a locked building. An apartment burglary, for example, might generate the following concealed information question: "A piece of jewelry was taken during the crime. If you are the guilty person, you know what that jewelry was. Was it A) a silver earring, B) a pearl necklace, C) a diamond ring, D) a gold bracelet, or E) a gold cross and chain?" It is hypothesized that a guilty individual will respond differently to the correct (relevant) alternative. Innocent suspects, due to their lack of specific knowledge about the crime, should respond fairly equally to each of the five alternatives.

TYPES OF TESTS

The four types of questions outlined above form the basis of the three different polygraph testing techniques: the Relevant/Irrelevant Technique (R/I), the Control Question Technique (CQT), and the Guilty Knowledge Technique (GKT).

Each has its strengths and weaknesses, and each works best under specific conditions. Therefore, you should anticipate which technique you will most likely

encounter in order to be adequately prepared on the day of the test.

The Relevant/Irrelevant (R/I) Technique

The R/I Technique was once the most frequently used form of lie detection in the United States. It was commonly exploited by personnel directors for pre-employment screening interviews, and had what was probably the broadest potential of the three techniques. That has changed.

In 1988, Congress passed a law (HR1212) called the "Polygraph Protection Act." Among other things, it made it illegal to use polygraph examinations for preemployment screening unless the employer is hiring for potentially dangerous or security-sensitive work. Pharmaceutical companies, for example, are excluded, as are security-type companies that are hiring night watchmen, armored car drivers, etc.

So far, HR1212 has driven a number of polygraph companies out of business, and it has forced budget cutbacks and wholesale employee terminations in those that wish to survive. There is still a possibility, however, that you will have to undergo an R/I test, especially if you want to work for the government.

As the name implies, the R/I Technique uses only two types of questions: relevant and irrelevant. According to R/I theory, deceptive individuals will show greater reactions to the relevant questions, while nondeceptive individuals, having nothing to fear, will show similar patterns of reactions to all the questions. To say that this technique is flawed is an understatement. First of all, most people have no trouble differentiating between relevant and irrelevant questions, so both innocent and guilty individuals have a high probability of responding differently to the relevant questions. If the guilty and innocent alike respond strongly to relevant questions, what is driving this

response? Perhaps it is surprise over the question or anger that the question is being asked. A variety of emotions could account for an elevated response.

Despite these flaws, the R/I test has its proponents, and it is still commonly used. In screening examinations, relevant questions will generally pertain to past job behaviors as well as current job qualifications. The following are some of the relevant questions usually used in preemployment screening tests. (Be sure to note how many of these could be control questions in a different situation.)

Q. Did you falsify any information on your application?

Q. In the last five years, did you ever steal any money or merchandise from a previous employer?

Q. Have you ever been fired from a job?

Q. Are you seeking a job with this company for any reason other than legitimate employment?

Q. Since the age of eighteen, have you ever been convicted of a crime?

Q. Have you used marijuana in the last ____ years?

Q. Have you used any other narcotic illegally in the past ____ years?

Q. Are you seeking a permanent position with this company?

Q. Have you deliberately lied in answering any of these questions?

The R/I Technique is used by employers as an aperiodic honesty check as well. Although most employers use honesty checks to determine the extent of employee theft or on-the-job drug use, others like to assess such things as employee satisfaction and commitment. Aperiodic honesty checks are composed almost entirely of relevant questions; apparent deception to any of the items is usually explored

further. Some questions that have been used in aperiodic honesty checks are:

Q. Are you satisfied with your present job and working conditions?

Q. Do you consider yourself to be a loyal company employee?

Q. Are you aware of any specific employee dissension?

Q. Have you ever witnessed a fellow employee deliberately damaging company property?

Q. Do you have any unauthorized keys?

Q. Do you intend to stay with this employer?

Q. Have you ever stolen merchandise from this company?

Q. Do you know any employee who has been revealing company secrets to a competitor?

Q. Have you ever put merchandise in the trash for later pickup?

Q. Do you suspect another employee of stealing from this company?

The Control Question Technique (CQT)

As polygraph theory evolved and the problems with the R/I Technique began to surface, a new test was developed. Both the relevant and irrelevant questions were retained, but a control question was added to the mix. As discussed above, control questions are designed to cause arousal in both nondeceptive and deceptive individuals. They usually probe for past misdeeds of the same general nature as the crime being investigated. Because it is assumed that we have all committed a few minor transgressions throughout our lives, truly innocent suspects are supposed to be more doubtful or concerned about the control questions than the relevant questions. This concern is thought to be reflected in higher peaks on the polygraph chart around

the control question areas. Guilty suspects, on the other hand, should show higher peaks around the relevant question areas—a reflection of their concern toward the relevant details of the crime. Many control questions cover a long period of time ("Before the age of eighteen, did you ever commit a serious crime?"), which is intended to make the suspect even more doubtful about the truthfulness of his answers. After all, who can remember every possible misdeed he might have committed over eighteen years?

Believe it or not, you yourself play a part in making the control questions so anxiety-arousing. During the informal interview that precedes nearly every polygraph exam, the examiner will develop and review all the test questions with you so that "there will be no misunderstandings during the actual test." Actually, you are being carefully manipulated to either A) be deceptive in answering the control questions, or B) be so concerned about your recollections that you become overly anxious.

Here's how it works: the examiner will pose a very broad question during the pretest interview, such as, "Have you ever stolen anything in your life?" Most people will sift through a lifetime of recollections in search of an instance where they might have stolen something. Now, consider the two ways you can answer this question. If you say "yes," you run the risk of letting the examiner know you have stolen in the past, which could easily prejudice his opinion of you. On the other hand, if you answer "no," you will worry that the examiner doesn't believe you and will assume that you are hiding something. Consequently, most people will admit to "small crimes"—taking pens home from work, stealing pocket change as a child, etc. This is exactly what the examiner wants you to do. He will dismiss these small crimes as being inconsequential and rephrase the original question: "Other than what we have discussed, have you ever stolen

anything in your life?" Now the anxiety can set in. Straight arrows who really haven't stolen anything will worry that they may have overlooked something; those who have committed real crimes (but didn't admit to them) will worry because they are forced to lie.

Either way, the polygrapher wins. He has gotten you to provide an elevated response to the control question, which he can then compare with the relevant questions. You fell into his trap. The polygrapher, of course, will not tell you that this manipulation is taking place. He will stress that each question must be answered completely with a simple yes or no response and that the machine will record any doubts or misgivings. He will try to persuade you that he only wants you to tell the truth. In reality, though, the examiner is counting on you to be moderately doubtful or intentionally deceptive. This is accomplished by making the control questions vague and difficult to answer with an unqualified "no."

It is debatable whether the addition of control questions makes a polygraph test any more valid. The polygraph industry thinks so, but one man who doesn't is University of Minnesota psychologist David T. Lykken. He argues that anyone formulating questions for a CQT must make three important assumptions about the examinee (Lykken, *Nature*, 1984, p. 684): 1) The subject will answer deceptively several questions referring to his or her past. Lykken argues that some people really have led lives of utmost integrity, so these control questions could not serve their intended purpose. 2) A subject who can answer the relevant questions truthfully will be more disturbed by the controls than the relevant questions. Lykken argues that it is unreasonable to predict with any confidence which questions a person will find more disturbing. 3) Guilty persons, who must answer relevant questions deceptively, will show stronger reactions to the

relevant questions than the controls. Lykken again argues that we really don't know which questions a person will find more disturbing.

The Guilty Knowledge Technique (GKT)

This test is the least likely to be encountered. Lykken first proposed this technique in 1959, but it has never really been accepted by the polygraph industry. The fundamental difference between the GKT and other techniques is that a GKT interrogation attempts to detect the presence of guilty knowledge—not lying. For example, in the burglarized apartment scenario mentioned earlier, an innocent person should respond fairly equally to each of the five alternatives (silver earring, pearl necklace, diamond ring, gold bracelet, or gold cross and chain) and would have only one chance in five of reacting most strongly to the correct alternative (i.e., actual item of jewelry stolen). With ten multiple choice items of this type, an innocent person would have less than one chance in ten million of reacting most strongly to all ten correct alternatives if he or she did not possess guilty knowledge.

Some people want the GKT to take the place of the CQT. One advantage is that it may reduce the number of false positives—innocent persons labeled guilty—because it would be almost statistically impossible for an innocent person to coincidentally react to the correct alternative enough times to achieve a “guilty” determination from an examiner. Unfortunately, say the GKT’s critics, this is a double-edged sword because the GKT also fails to detect a large number of guilty suspects. Critics also complain that the GKT may not be widely applicable. It obviously could not be used as a preemployment screening test.

Other oft-mentioned problems with the GKT are the concept of “guilty” knowledge and the difficulty in making the test valid. Concerning the former, critics

charge that knowledge about an incident may not differentiate between a guilty and an innocent person where, for example, a suspect is present at the scene of a crime but claims someone else did it. Also, the test becomes useless when the press covers a sensational crime in such a way that all the relevant details become public knowledge. When addressing the latter issue, many police investigators/polygraphers claim that it is just too difficult to come up with enough good questions about a crime to clearly implicate a suspect. Furthermore, they say, if enough information is obtained to create a six- or ten-item GKT test, there is still no guarantee that the suspect will not claim to have had these facts revealed to him in other parts of the investigation—or that the suspect will even remember such details in the first place.

All things considered, you probably do not have to worry about being subjected to a GKT exam. The polygraph industry doesn't like it, so it is rarely used. Instructions for beating a GKT will still be presented in the countermeasures section, just in case you face that occasional polygrapher who favors the procedure.

PRACTICE TESTS

The following pages contain practice tests for R/I, CQT, and GKT polygraph exams. Each begins with a short scenario, which you should read and imagine to be actually occurring in your life. For the R/I test, try to determine whether each question is relevant (R) or irrelevant (I). For the CQT test, try to label each question as relevant (R), irrelevant (I), or control (C). Answers are provided at the end of the chapter. Later, after you have read the section on countermeasures, you can come back to these tests and practice your skills.

Although it is not necessary, you may find it useful to practice with a friend. Try to mimic a real-life

polygraph setting as much as possible. The more you practice, the better prepared you will be. All the GKT test questions are relevant, so there is not much to be gained by going over these tests until you have read the section on countermeasures. A word of warning: GKT tests favor innocent suspects, so, if you are innocent, the best countermeasure is to be yourself. If you are guilty, then you should know that the GKT can be very hard to beat, especially if you have a good memory for detail and remember exactly how the crime was committed. Practice of your countermeasures is essential.

R/I Scenario

You have applied for an entry-level position of Quality Control Analyst at ABC Pharmaceuticals, a midwestern pharmaceutical wholesaler. Although your work history and résumé are well above average, the personnel director has asked you to submit to a polygraph examination because your job will put you in constant contact with a variety of drugs. Because this is a preemployment screening examination, there is no pretest interview. The examiner has you wired up and is ready to begin.

Questions

R or I

- | | |
|---|-------|
| 1. Is today Tuesday? | _____ |
| 2. Are you sitting in a chair? | _____ |
| 3. Have you ever stolen merchandise from a place where you've worked? | _____ |
| 4. Have you ever consumed alcoholic beverages while on the job? | _____ |
| 5. Is your mother's name Sarah? | _____ |
| 6. Do you live in an apartment? | _____ |
| 7. Have you ever been convicted of a crime? | _____ |
| 8. Was it raining this morning? | _____ |
| 9. Have you ever smoked marijuana on the job? | _____ |

10. Are you wearing glasses? _____
11. Do you consider yourself trustworthy? _____
12. Do you have red hair? _____
13. Have you ever been through an alcohol or drug treatment program? _____
14. Do you watch television? _____
15. Thus far, have you deliberately lied to any of the questions I have asked you? _____

CQT Scenario 1

You work on the dock unloading trucks for A.A. Blair's, a chain of five discount department stores. Business couldn't be better. Christmas sales were far above projections, and everyone's morale is high. Unfortunately, there has been some whispering around the water cooler that a lot of merchandise cannot be accounted for.

The year-end inventory confirms the bad news—there is more than ten thousand dollars worth of merchandise on the books that is not in the warehouse. Some have suggested that a driver is working with one of the dock workers to defraud the company.

The store manager conducted interviews with all the dock personnel, but no one was talking. Reluctantly, the manager brought in a polygrapher to handle the problem. Everyone so far has passed, and you are about to begin your test.

Questions

R, I, or C

1. Are you one hundred years old? _____
2. Is your name Scott? _____
3. Have you ever "covered" for a fellow employee by falsifying his/her time card? _____
4. Have you ever falsified inventory records for personal gain? _____
5. Were you born in Baltimore? _____

6. Have you ever stolen merchandise from this company? _____
7. Do you drink coffee? _____
8. Do you know of anyone who is trying to defraud this company? _____
9. Do you have any children? _____
10. Have you falsified your employment application in any manner? _____
11. Have you ever hidden merchandise in the trash to be picked up later? _____
12. Are your parents divorced? _____
13. Have you ever called in sick when actually you were not? _____
14. Do you work on a dock? _____
15. Have you ever tried to defraud this store in any manner? _____

CQT Scenario 2

After three years of hard work, you have finally been named senior administrative assistant to the chairman of the Bart County School Board. There were three other candidates competing for the position, but your knowledge of the county's computer systems pushed you over the top.

Not long after you began work at your new position, strange things started to happen. Computer files were being wiped out, programs wouldn't run correctly, and the department's specialized financial software was subjected to two different viruses.

The department heads were convinced that all this vandalism was performed by a disgruntled employee. Unfortunately, most of the department's employees have limited access to the computers—your access is unlimited and totally unsupervised. Although there is no logical reason for you to be behind this wave of vandalism, you are the first to be administered a polygraph exam by the county police.

Questions**R, I, or C**

1. Do you have a sister? _____
2. Before the age of eighteen, did you ever purposefully manipulate another person's software? _____
3. Have you ever used the department's computers for unauthorized purposes? _____
4. Are both your feet on the floor? _____
5. Do you know who is sabotaging the department's computer records? _____
6. Does one plus one equal three? _____
7. Are you wearing a shirt? _____
8. Have you ever made or received personal phone calls while on company time? _____
9. Are you happy in your present position? _____
10. Are your eyes brown? _____
11. Do you know how to drive? _____
12. Have you ever suspected a fellow employee of being under the influence of alcohol while on the job? _____
13. Do you know of people who are dissatisfied with their employment in the department? _____
14. Are you right-handed? _____
15. Have you ever planted a computer virus in the department's computer system? _____

GKT Scenario

An apartment has been burglarized. While not admitting your guilt, you know that the apartment was #112 and that the following items were taken: cash, credit cards, a diamond ring, a Minolta camera, a pair of binoculars, a stamp collection, an electric guitar, and a tennis racket. You also know that the cash was hidden in the back of a clock and that the clock was deliberately broken. You have been arrested for the crime and are about to take a GKT polygraph exam. After the detective reads each alternative, you must repeat it and deny that

it is the correct alternative (e.g., "231. No.")

Questions

1. If you are guilty of this crime, then you know the number of the apartment that was burglarized. Was it:

- a) 418
- b) 206
- c) 112
- d) 327
- e) 530

2. The cash stolen from this apartment was in a unique hiding place. If you are the guilty person, then you know where the cash was hidden. Was it:

- a) behind a picture
- b) under a trash can
- c) inside a medicine cabinet
- d) inside a clock
- e) inside an album cover

3. Something that was on the speaker close to the chair in the living room was stolen. If you are the guilty person, then you know what was stolen. Was it:

- a) a lamp
- b) a book
- c) a brass urn
- d) a pair of binoculars
- e) a jewelry box

4. A musical instrument was stolen from the apartment. If you are the guilty person, you know what that instrument was. Was it:

- a) a saxophone
- b) a guitar
- c) a harmonica
- d) a flute
- e) a violin

5. Something valuable was taken from the dining room table. If you are the guilty person, then you know what this was. Was it:

- a) a television
- b) an antique clock
- c) a stamp collection
- d) a gold pen
- e) a pair of silver candlesticks

6. Some jewelry was stolen from the apartment. If you are the guilty person, you know what was stolen. Was it:

- a) a silver bracelet
- b) a pearl necklace
- c) a pair of jade earrings
- d) a gold cross and chain
- e) a diamond ring

7. Something was stolen from a wallet found in the apartment. If you are the guilty person, then you know what was stolen from the wallet. Was it:

- a) a driver's license
- b) a key
- c) money
- d) credit cards
- e) a traveler's check

8. Something was deliberately broken during the commission of the crime. If you are the guilty person, you know what was broken. Was it:

- a) a trophy
- b) a clock
- c) a bottle
- d) a lamp
- e) a picture frame

9. A camera was stolen from the apartment. If you are the guilty person, you know what brand it was. Was it:

- a) a Toshiba
- b) a Nikon
- c) a Canon
- d) a Minolta
- e) a Pentax

10. Some sporting equipment was taken from the apartment. If you are the guilty person, you know what was taken. Was it:

- a) a stopwatch
- b) a tennis racket
- c) a skateboard
- d) a bowling ball
- e) a baseball glove

Answers

R/I Scenario

- 1. I
- 2. I
- 3. R
- 4. R
- 5. I
- 6. I
- 7. R
- 8. I
- 9. R
- 10. I
- 11. R
- 12. I
- 13. R
- 14. I
- 15. R

CQT Scenario 1

- 1. I
- 2. I
- 3. C

- 4. R
- 5. I
- 6. R
- 7. I
- 8. R
- 9. I
- 10. C
- 11. R
- 12. I
- 13. C
- 14. I
- 15. R

CQT Scenario 2

- 1. I
- 2. C
- 3. R
- 4. I
- 5. R
- 6. I
- 7. I
- 8. C
- 9. R
- 10. I
- 11. I
- 12. C
- 13. C
- 14. I
- 15. R

CHAPTER FIVE

COUNTERMEASURES



"The whole procedure requires that the subject cooperate."

—R. Decker, Chief of the Federal Government's Polygraph Trainers

"If you can control your bowels, you can control your test results."

—Douglas Gene Williams, a former Oklahoma police polygrapher who now campaigns against the lie detection industry

A polygrapher's job would be so much easier if every suspect behaved like an unknowing lamb being led to slaughter. Most Americans, however, will not sit idly by while someone tries to tamper with their rights—like the right to hold down a job or the right to be treated with dignity and respect. Professional polygraph examiners hope that you never read this book—and especially this chapter—because it represents a challenge to their multimillion-dollar industry. Like a con man, the polygrapher counts on your gullibility and ignorance in order to trick you into believing his machine can magically read your thoughts.

It's time for us to stop bowing down to their Orwellian creation and fight back! It's time to make a liar of the lie detector! You took the first step in limiting a polygrapher's power over you by

opening this book. The sole reason for this book's existence is to demythologize the lie detector and give you a clearer understanding of how it works—or doesn't work. I hope you spent some time going over the practice tests in the last chapter because the single most important skill you can develop to beat a lie detector test is the ability to recognize and differentiate between relevant questions, irrelevant questions, and control questions. Once you feel confident in recognizing these question categories, you can move on to countermeasures.

Countermeasures are deliberate techniques used by individuals to alter their response patterns during a polygraph examination. The list of countermeasures has grown over the years, but they all fall into three major categories: physical, cognitive, and pharmacological.

PHYSICAL COUNTERMEASURES

Because a polygrapher must infer deception from a pattern of physiological responses, any physical activity that alters a physiological response is a potential countermeasure. The trick is to know when you should enhance your responses so that you appear to be nervous (during control questions), and when you should attenuate your responses so that you appear to be calm and relaxed (during relevant questions). The following list of physical countermeasures contains a variety of popular techniques. Many have been used in university studies assessing polygraph validity.

Breathing

If you want to appear calm and truthful, you should breathe at a calm, regular pace. A polygraph chart will indicate nervousness/deception if you deviate from a slow, regular pattern in any of the following ways: inhaling deeply, breathing in shallow and erratic gasps,

momentarily holding your breath, sighing, breathing rapidly through your nose, panting with your lungs full, or gasping with your lungs empty.

Muscle Tension

To appear truthful, you should sit calmly and literally not move a muscle. You can then elevate your responses to the control questions by tensing and relaxing any of the major muscle groups (arms, thighs, abdominals, and gluteus). Note: If you are going to tense your arm as a countermeasure, do not tense the arm that has the blood pressure cuff attached. This is too easily detected. Also, you may want to try pressing your arm hard against the chair's arm (most polygraph examiners require you to sit in an armchair) because that is harder to spot than flexing your biceps. Another very effective trick is to pucker up your anus for five to ten seconds and then release. This creates a momentary elevation of blood pressure that the examiner will believe is being caused by anxiety at a particular question.

One word of caution regarding these muscle techniques: polygraph examiners have developed a counter-countermeasure to limit their effectiveness. Sometimes called a pneumatic chair or pressure chair, it consists simply of a chair with pressure sensors or strain gauges in the arms and seat. These sensors are attached to a separate pen on the polygraph that will record any unnatural muscle tension. Should you suspect that you are sitting in one of these chairs, you should alter your game plan and focus on the nonphysical countermeasures.

Pressing the Toes

Unlike tensing a major muscle group, pressing the toes against the floor usually will not be detected by a specialized chair. To appear that you are experiencing

anxiety in response to a particular question, all you need to do is press your toes hard against the floor for a few seconds and then release. Polygraphers have developed a counter-countermeasure for this technique as well, and it consists of nothing more than having you place your feet on a footrest for the duration of the examination. Some examiners may even ask you to remove your shoes.

The Hidden Tack

As you can imagine, pressing your toe against a tack, even fairly lightly, will cause a violent deflection in the polygraph needles. And if you suffer from ingrown toenails or blisters, you don't even need the tack; light pressure against the sore spot will achieve the same result. I even know of one person who deliberately cut his big toe the day before his test so that he didn't have to bother with the tack!

Biting the Tongue

Obviously, you should not try to bite your tongue while responding to a question. Immediately after you have answered, though, you should bite down hard for a few seconds and then release. Make sure to keep a straight face.

Shifting Positions

Shifting position in your chair can be tricky. You do not want to shift positions a number of times during the test (it looks like you're squirming). What you are trying to accomplish is a short, quick, unsuspecting shift. One technique is to begin the test by sitting up straight and then gradually leaning forward as the test progresses. When you get to a control question where you want to appear overly anxious, quickly shift so you are sitting up straight again. I would only try this once during the test because polygraphers are trained to be

suspicious of anyone who exhibits a lot of extraneous physical motion.

Antiperspirant

There is some anecdotal evidence suggesting that a little antiperspirant on your fingertips will neutralize the GSR needle on the polygraph. This may be true, but don't go overboard with the antiperspirant. Remember, the polygrapher will be able to feel your fingertips when he applies the GSR electrodes. If he suspects you've doctored your fingertips, he may ask you to wash your hands before the test. Clear fingernail polish has been suggested as an alternative to antiperspirant, but it is much more easily detected.

Coughing, Sneezing, and Yawning

Don't waste your time with these. Everybody knows you can wipe out a polygraph test by coughing after every answer, but that would look a little ridiculous. Even if you try it only a few times, you still will not be getting away with anything. Any polygrapher worth his salt will make a notation on the chart whenever you cough, sneeze, or yawn, and he'll just disregard that response. What's more, if you cough or yawn a lot, the examiner will suspect that you are trying to pull a fast one on him and start looking for other indications that you may be using countermeasures.

APPLICATIONS OF PHYSICAL COUNTERMEASURES

With the R/I test, you are expected to show an elevated response to one or two relevant questions because everyone is assumed to have done things in their lives that they would rather not admit. The polygrapher will focus on these few areas for the

remainder of the test. Your plan should be to use a physical countermeasure (that is, show an elevated response) on one or two questions about which you really have no worries. Your goal is to get the examiner to focus in on these areas and leave more potentially damaging areas of your life alone.

The CQT test is where your knowledge of question categories is all-important. You must be able to separate the control questions from the relevant questions and always show an elevated response to the control questions. *You cannot be judged deceptive if your responses to control questions are greater than or equal to your responses to relevant questions. Never forget this.*

Start by separating the control questions from the relevant questions during the pretest interview. When the test starts, sit calmly and breath regularly during all the relevant questions and use a countermeasure during all the control questions. You would be better off to use a series of different countermeasures so that your elevated responses don't have the same characteristics time after time. For example, try shallow breathing and a toe press during the first control question, pressing on a tack and a deep breath during the second, and biting the tongue hard and puckering the anus during the third.

Believe it or not, many polygraphers will only catch the most obvious and overt attempts at countermeasures. They simply do not expect you to have a sophisticated plan laid out in advance. This is a great advantage to you. As long as you don't get careless and sloppy, none but the very best examiners will have any idea that you've suckered them.

Because the GKT can only be used for specific incidence cases (i.e., after a crime has already been committed), innocent suspects don't need to learn any countermeasures. After all, an innocent person couldn't

possibly know which items were filler and which were relevant. Consequently, as an innocent person, you are protected by this technique because 1) not knowing which items are relevant, you should show a fairly similar pattern of responses across all the items, and 2) even if you showed an elevated response to some of the items, it would be almost statistically impossible for you to coincidentally respond to enough critical items to put yourself in jeopardy. If you are guilty of a crime, however, then you need to know how to use these physical countermeasures to avoid being detected.

Some would argue that I shouldn't reveal this information because the guilty should be caught and punished. I have no desire to see thieves, muggers, rapists, and murderers getting off for crimes they have committed. My desire for revenge, however, is tempered by my desire to live in a world where people are not unjustly charged and convicted. I believe polygraph machines are unreliable and dangerous, and I hate to see one used to make a case for or against any person. If a person is indeed guilty, then there are more effective ways to prove it than charting how much he sweats or how rapidly he breathes.

That said, the best way I know of to neutralize a GKT exam is to dampen your responses to all of the items (see the sections on cognitive and pharmacological countermeasures), or to selectively elevate responses throughout the test. Because most GKT test questions have five or more alternatives, get a piece of paper and write the numbers 1 through 5 at the top of the page. Then write the numbers 1 through 10 in a column along the left-hand margin. Now, randomly choose one of the five numbers at the top and write it next to #1 in the left-hand column. An easy way to assure randomness is to roll a die and record whatever number comes up. If you roll a 6, just roll again.

Keep doing this until you have ten randomly chosen

numbers in the left-hand column. A typical sequence might be: 2, 5, 2, 4, 3, 5, 3, 4, 4, 1. Memorize this sequence. Then, when you are being tested, use the physical countermeasures to elevate whichever alternative is called for by your memorized sequence. If there are more than ten questions, just repeat the sequence over again until the test is finished; if there are less than ten questions, just start over at the beginning of your sequence for each repetition of the test.

The logic behind this technique is that you are imitating the thought processes of an innocent person by having elevated responses in an apparently random fashion. An innocent person couldn't possibly know which items are relevant, so his elevated responses should have no discernable pattern, and he stands a good chance of hitting at least one relevant alternative simply by coincidence. Your random sequence of numbers accomplishes the same thing. The only drawback to this technique is that it takes a lot of practice. I am confident, though, that the possibility of a prison term will serve as ample motivation.

COGNITIVE COUNTERMEASURES

Unlike physical countermeasures, cognitive countermeasures are impossible to detect—even by the most experienced examiners. As mentioned earlier, the polygrapher is relying on your ignorance and gullibility and expects your driving motivation is to tell the truth. When you use a cognitive countermeasure, telling the truth becomes secondary to altering the way in which you perceive the test.

Hypnosis/Biofeedback

The jury is still out about the effectiveness of hypnosis and biofeedback to appreciably alter a polygraph test's results. Some say hypnotic suggestion

(e.g., hypnotically suggested amnesia) is an effective countermeasure. Others say it is just a waste of time. Biofeedback, on the other hand, has long been used to lower blood pressure and ease stress. Hard-driving Type A personalities, whose lives are characterized by stress, are especially receptive to the calming effects of biofeedback. This has led some researchers to theorize that biofeedback might also help to lower blood pressure in normal individuals during specific stressful situations (such as a lie detector test).

The research in this area looks promising. In fact, subjects have been taught not only how to lower their blood pressure, but how to significantly lower their GSR levels as well. That's two out of three of the major physiological measures used in a polygraph exam! The only drawback to biofeedback (and hypnosis) is that it costs a lot of money and takes a lot of practice to achieve any measurable reductions. One alternative would be to invest in one of the relatively low-cost biofeedback monitors advertised in high-tech mail order catalogs and the backs of magazines (*Psychology Today* and all the new age and health magazines usually run at least one ad for this type of equipment every month). There is no reason you shouldn't be able to get the same results at home as others who have spent a fortune on high-priced clinical workshops.

Thought Control

No, this does not refer to some covert CIA operation. Thought control is simply an individual's conscious effort to alter his or her perceptions of reality. Once again, the ability to differentiate between the three question categories is essential. The basic procedure is to dissociate yourself from the relevant questions and heighten your response to the control questions. For example, when the polygrapher asks you

the relevant question, "Did you steal the three hundred dollars from the cash register," you would concentrate on peaceful thoughts like the crashing surf, a lazy Sunday afternoon on the lake, or anything else that takes your mind off the question.

Alternatively, when asked a relevant question, you can convince yourself that the question means something other than what was intended. The question "Have you ever consumed alcoholic beverages while on the job" could, for example, be rationalized as follows: "Well, I have been hiding a bottle of whiskey in the rest room and drinking it there . . . but when I'm in the rest room I'm not really 'on the job' . . . so no, I've never consumed alcoholic beverages while on the job." Responses to control questions could similarly be elevated by disregarding the question and focusing on stressful thoughts like what would happen if you were to lose your job, go to jail, total your car on the way home, be audited by the IRS, and so on.

To date, only one researcher has attempted to test this technique. In a laboratory study of polygraph examinations, this researcher recruited a group of method actors from his school's drama department and told them that they should apply their acting skills to appear innocent during the polygraph exam. Every actor was detected. This was not really a fair experiment, however, because the design was flawed. You see, the experimenter had only told the drama students to *act* innocent during the polygraph exam. He had not given them any training about how to tailor their responses to particular questions or about how a polygraph exam goes about detecting deception. With the knowledge you have already accumulated, you would stand a much better chance against a trained polygraph examiner than any of these method actors.

Results Feedback

It has long been proven that school children will make better grades on weekly tests if they know how they did on the previous week's test. The same seems to be true for polygraph exams. If you have had to undergo polygraph exams in the past and you were not judged deceptive, you stand a better chance of passing future polygraph exams than someone who has never taken one. Remember when your parents told you that practice makes perfect? Here's another example that shows they were right.

Belief in the Machine

The final cognitive countermeasure is really a frame of mind or pattern of thinking that underlies everything else in this book: belief in, or skepticism toward, the machine. If you believe the polygraph machine can detect your deceptions, it will. If, on the other hand, you are confident that the polygraph machine is no more able to weed out lies than snake oil can cure cancer, you will avoid detection. Several university researchers have accumulated evidence supporting this theory by conducting what is known as "bogus pipeline" research.

Bogus pipeline theory proposes that when subjects believe that their attitudes are detectable by a physiological recording device, they more readily express their actual attitudes. The problem facing the university researchers was to convince the skeptical college student that the polygraph machine actually works. They accomplished this by presenting the subject with an impressive display of electronic gadgetry and promoting it as a new kind of super lie detector capable of detecting even the smallest physiological changes. ("Bogus pipeline" refers to all the wires, relays, and displays that are purportedly used to detect deception. In reality, all this sophisticated gadgetry has

nothing to do with lie detection—it is intended to intimidate the subject. All style, no substance.) Subjects deceived in this way have been found to admit to more socially undesirable responses, such as negative attitudes toward handicapped people. The researchers claim these confessions are evidence that the bogus pipeline can bring about a higher level of “truthfulness.”

The significance of this research for our purpose is that if the validity of polygraph testing is dependent upon the subject's belief in the effectiveness of the machine, then a possible countermeasure would involve training people to believe that the polygraph does not work. Simply put, your goal is to go into the exam with the utmost skepticism. The more dubious you are of the polygrapher's claims, the more difficult it will be for him to trip you up.

APPLICATIONS OF COGNITIVE COUNTERMEASURES

Your best defense against the R/I Technique is to go into the exam with the strongest possible belief that the machine doesn't work and cannot harm you. You can supplement this by thinking peaceful thoughts during the relevant questions that concern you and thinking stressful thoughts on one or two relevant questions that do not cause you any concern. Your goal is to get the examiner to shift the focus of the test to those areas about which you are not really worried. Once you see him moving in that direction, however, you stop elevating your responses and begin thinking peaceful thoughts again.

As mentioned before, the way to beat a CQT is to elevate your responses to control questions and attenuate your responses to relevant questions. Once again, you need to go into the test with the proper frame of mind (i.e., skepticism) and use the peaceful

thoughts/stressful thoughts technique discussed above. You can also try hypnosis and biofeedback if you are so inclined and have the money.

For the GKT, innocent suspects don't need countermeasures. Guilty persons, on the other hand, may want to seriously consider all the cognitive countermeasures available. Should you use the controlling thoughts countermeasure, apply the random numbers sequence discussed under physiological countermeasures. This time, however, think stressful thoughts whenever the preselected random alternative comes up and try to dissociate yourself from all the other alternatives presented. Practicing with a biofeedback monitor would help you assess how quickly you can switch from a peaceful to a stressful frame of mind and back again.

PHARMACOLOGICAL COUNTERMEASURES

In contrast to physical countermeasures, which may be detected by an observant polygraph examiner (either by noticing unusual behaviors or running multiple polygraph charts), the use of various pharmacological agents, or drugs, may be more difficult to detect. The downside of these techniques is that current research on the effectiveness of drug countermeasures is not very promising. In fact, ingesting a drug before you take a polygraph exam may be the worst thing you can do. Douglas Gene Williams, a former Oklahoma police polygrapher who since 1978 has conducted a personal campaign against lie detectors, advises anyone who is about to take a polygraph exam to stay away from drugs. He argues that you need to keep your wits about you during an examination—drugs will only dull your senses and cause you to become confused and make mistakes.

Some of you, however, have probably heard

fantastic tales about how someone took some miracle drug and passed a lie detector test with flying colors. There are some substances that may help.

Warning: The following section on drug usage is for information purposes only. Neither the publisher nor the author encourages or endorses the use of drugs or other controlled substances without a proper prescription. Some of the drugs listed may have dangerous and even life-threatening side effects. Consult a physician before attempting to use any of these medications.

The drugs most commonly used to escape detection are the classical sedatives and a special class of tranquilizers called ataractics. As their name implies, sedatives are calming agents that allay anxiety and lower the level of tension. The major drawback of sedatives is that they are nonselective: not only do they lower autonomic responses (GSR, blood pressure, breathing rate), but they also affect overt psychomotor behaviors. In other words, the subject's responses on the polygraph chart would flatten out, but so would the subject himself. Concentration would be reduced, reaction time would be slowed, and a mild hypnotic effect would most likely be experienced. These symptoms are easy to spot, and no polygrapher in the world would administer a polygraph exam to someone who appeared to be doped up. That brings us to the ataractics.

Ataractics are compounds with a tranquilizing effect, which is to say they are sedative in nature. But the influence of ataractics is limited more to the subcortical systems (more specifically, the reticular formation, which controls the sleep/wake cycle) and the limbic system. Consequently, unlike classic sedatives, ataractics will have little influence on clarity of consciousness and intellectual performance. In other words, the subject's autonomic nervous system will be mildly sedated, but he or she won't appear to be doped up to the examiner.

Commonly Prescribed Ataractics

GENERIC NAME: Chlordiazepoxide hydrochloride

CATEGORY: Schedule IV controlled substance

COMMON BRAND NAMES: Librium, Corax, Libritabs, Protensin, Sereen, Tenax, Zetran

DOSAGE: Daily oral dose is 10-50 mg.

ONSET AND DURATION: 1-2 hours onset; up to 24-hour duration

SIDE EFFECTS: Lethargy, nausea, abdominal discomfort, transient hypotension (low blood pressure)

PARTICULARS: Chlordiazepoxide was introduced in clinical psychiatry in 1960. Its side effects after oral administration are slight, but it may cause psychomotor weakness. This drug should never be taken with alcohol, and it is not recommended for day-to-day use.

GENERIC NAME: Diazepam

CATEGORY: Schedule IV controlled substance

COMMON BRAND NAMES: Valium, Levium, Stesoloid, D-Tran, Erital

DOSAGE: Daily oral dose is 6-30 mg.

ONSET AND DURATION: 1 hour onset, up to 24-hour duration

SIDE EFFECTS: Lethargy, nausea, abdominal discomfort, transient hypotension

PARTICULARS: Diazepam has a more marked sedative and hypnotic effect than chlordiazepoxide. Intense drowsiness can be a problem, especially when it is taken for the first time. Although easily available, diazepam is not a good choice for a pharmacological countermeasure. It is likely to cause drowsiness, clumsiness, or slurred speech, which will quickly tip off a competent polygraph examiner that a subject is under the influence of some drug.

GENERIC NAME: Meprobamate

CATEGORY: Schedule IV controlled substance

COMMON BRAND NAMES: Equanil, Miltown, Sedapon, Arcoban, Meribam, Saronil

DOSAGE: Varies widely. The average daily dose is 400-1200 mg., but doses up to 2-3 grams are tolerated.

ONSET AND DURATION: Begins therapeutic action in 1 hour; peaks in 2-3 hours; half-life of about 10 hours

SIDE EFFECTS: Drowsiness, dizziness, slurred speech, headache, hypotension, nausea, palpitations

PARTICULARS: Prior to the introduction of chlordiazepoxide, meprobamate was by far the most popular ataractic. It derives from mephenesin, a compound introduced as a muscle relaxant shortly after World War II. When it was found that mephenesin had sedative properties as well, efforts were made to alter the molecule so that duration and intensity of the sedative effect were enhanced. Meprobamate was the result. Meprobamate is one of the few drugs to be scientifically tested and found to reduce the accuracy of polygraph examiners' judgments (Waid, Orne, Cook, and Orne, 1981).

GENERIC NAME: Propanolol

CATEGORY: Schedule IV controlled substance

COMMON BRAND NAMES: Inderal

DOSAGE: Daily dose is 40-160 mg.

ONSET AND DURATION: Can act as quickly as 1-5 minutes and have a 6-24 hour duration

SIDE EFFECTS: Fatigue, lethargy, hallucinations, hypotension, nausea, skin rash

PARTICULARS: Propanolol falls into a special class of ataractics known as beta-blockers. Though normally prescribed for hypertension, propanolol has also been found to be useful in combating incidental tensions produced by anticipation of stressful events (e.g., a midterm exam, a speech, a polygraph test). This drug is particularly effective when anxiety is manifested in

somatic symptoms (e.g., heart palpitations, nausea, diarrhea). Beta-blockers are quickly gaining a solid reputation as reliable pharmacological countermeasures.

GENERIC NAME: Atenolol

CATEGORY: Schedule IV controlled substance

COMMON BRAND NAMES: Tenormin

DOSAGE: Daily dose is 50-100 mg.

ONSET AND DURATION: Can act as quickly as 1-5 minutes and have a 6-24 hour duration

SIDE EFFECTS: Fatigue, lethargy, hallucinations, hypotension, nausea, skin rash, fever

PARTICULARS: Atenolol is a relatively new beta-blocker, but it is also commonly prescribed for individuals with transitory stage fright or performance anxiety. Other beta-blockers have also been found effective in anxiety syndromes with a strong somatic component. Two commonly prescribed medications are alprenolol (Aptine) and oxprenolol (Trasicor). The last compound, given in a single 40-mg. dose, has helped many professional actors overcome extreme cases of opening night jitters.

Getting the Drugs

Once again, I cannot stress enough that you should see a doctor if you want to try to use any of these drugs as polygraph countermeasures. Unfortunately, many conservative doctors may not want to prescribe a drug for you just so that you can beat a lie detector test. Therefore, you must have a good reason for needing the drug. Your best bet would probably be to tell your doctor that you have a major college exam coming up or that you have to make a major presentation in front of a large audience. Then tell him that in the past, you have gotten heart palpitations, nausea, and diarrhea whenever you had to face such a situation. Being able

to present the doctor with a list of physical components such as this is a must; if you only tell him that you "feel nervous," he may think you're overreacting and prescribe a placebo. A doctor will be much more likely to prescribe medication for "heart palpitations" than for "a nervous feeling."

Applying Pharmacological Countermeasures

Whether the polygraph exam is of the R/I, CQT, or GKT variety, the only way to apply a pharmacological countermeasure is to take the drug before the exam and hope for the best. All of the drugs outlined above will tend to flatten out physiological responses, which may or may not help. One likely outcome is that the test will be judged inconclusive and have to be taken some other time. In some instances, however, an inconclusive result is viewed as a *de facto* pass, and the test will not have to be taken again.

CONCLUSIONS

* Despite what the polygraph industry would have you believe, physical, cognitive, and pharmacological countermeasures are effective means of neutralizing most polygraph examinations. The risk of being caught is minimal, and the rewards for success can be substantial (like keeping yourself out of jail).

* If you never want to fear another polygraph exam, you must do two things: 1) learn how to differentiate between relevant questions, irrelevant questions, and control questions; and 2) practice, practice, practice. Pick out a few of the countermeasures that appeal to you and practice carrying them out without looking obvious. Then, get a friend and run through the sample tests at the end of Chapter 4. Make the situation as real as possible and have your friend look for any telltale signs of countermeasures that you may have missed.

The better you get in practice, the better you'll do if
and when you have to undergo the real thing.



CHAPTER SIX

THE DAY OF THE TEST



*"Any fool can tell
the truth, but it
requires a man of
some sense to know
how to lie well."*

—Samuel Butler

As with a dentist's appointment, a trip to a polygrapher's office is something most people dread. If you've ever had to take a polygraph exam, then you know the feelings that precede it: anxiety over not knowing what to expect; resentment over having to submit to such a procedure in the first place, and outright anger over the possibility that some stranger may brand you a liar. These feelings are quite normal, and you have every right to express them. But when you do, make sure it is only to friends and family, not to the polygrapher. All the adverse feelings you have toward either the machine or the examiner should be left at the front door when you leave your home in the morning.

BEFORE YOU LEAVE FOR THE EXAM

Put yourself in the proper mind-set for the ordeal that lies ahead. There are several things you should do to prepare yourself emotionally and psychologically.

Clothing is always important. Consider the following: A young man was arrested late one Friday evening for possession of marijuana. At the time of the arrest, the police officers had a great time making fun of his long, greasy hair, tie-dyed T-shirt, and dirty, torn blue jeans. But by the time his hearing came up, his entire appearance had changed. The hair was trimmed short and styled to perfection, and the tie-dyed shirt and blue jeans had given way to a three-piece Brooks Brothers suit. Obviously, someone (probably his lawyer) had told him that people who dress like bums are often discriminated against, but everyone forgives a clean-cut youth.

You should try to dress nicely for the exam. Rest assured that the examiner will be doing everything in his power to impart to you a professional demeanor. Men should wear a jacket and tie and remember to shave. Women should wear a tailored suit or skirt and blouse. Keep jewelry to a minimum and be conservative with makeup. T-shirts, jeans, tennis shoes, shorts, and jogging suits or sweats are definite no-no's. The whole idea is to take away any psychological advantage the examiner may have over you by being more professionally dressed. When choosing your outfit, you may want to go with loose fitting—not baggy—clothes (the better to conceal muscle flexing) and nonsqueaky shoes (and don't forget to hide the tack in your sock).

The last thing you should do before you leave for the exam is to take a brief inventory of your polygraph skills. Remember the four types of polygraph questions: relevant, irrelevant, control, guilty know-

ledge. Be certain you can differentiate between them. Go over the three polygraph exam techniques. Review your countermeasures. Do you have a "game plan" for their use? All of these things are important, and you should be able to recall all of them without hesitation. Remember—the polygraph examiner does this every day. You've got only one shot, so make the most of it.

ARRIVING AT THE EXAM LOCATION

Whether your exam is conducted at your place of employment, a downtown office building, a police station, or even in a hotel room, the cardinal rule is *be on time!* I cannot stress this enough. Your examiner will automatically interpret any lateness as a conscious or subconscious attempt to avoid or delay the test. Being late is a surefire way to raise suspicions in the examiner about some presumed hidden motives, so don't let him put a black mark beside your name before you even show up. If you are not sure of where the testing site is, make a few dry runs before the actual day of the test. Is there adequate parking? Will the early-morning rush hour or the lunchtime traffic snarls delay your arrival? Any lateness, no matter how small and no matter how unintentional or unavoidable, will be the first strike against you.

If you are lucky, your polygraph exam will be conducted either at your place of employment or in a hotel room. In the former case, the examiner is off his home turf and in surroundings with which you are more familiar. In the latter case, the turf is fairly neutral. He may be the one renting the room (a small psychological advantage), but hotel rooms are, by and large, nonthreatening, and you can get your own psychological edge by pointing out (gently) that a hotel room seems like a strange place to be doing such "important" testing. This puts the examiner on the

defensive immediately, because by noting the peculiarity of the surroundings, you have indirectly commented on his professionalism. No doubt he will try to save face by explaining to you that his office is being painted or that he has chosen this location for your benefit so that you don't have to drive so far. No matter what reason he gives, all he is trying to do is convince you that he is a professional and that the atypical surroundings will have no effect on the testing process.

If, on the other hand, your exam is conducted at a police station or in the polygrapher's office, then you are automatically at a disadvantage. You are on his turf, and he has probably manipulated the surroundings to make himself look like the ultimate professional. Don't be surprised to see a wall full of diplomas, certificates of achievement, awards, and so on, testifying to his abilities. This is a subtle psychological ploy often used by "professionals." A framed diploma is an excellent way for someone to say, "See how great I am" without uttering a word.

Another item you may notice in the office is an American flag. Ronald Reagan proved (as if there were ever any doubt) that you can get away with just about anything by wrapping yourself in the flag. A flag in the polygrapher's office subconsciously sends the message, "This guy is an American. He believes in American values and would never do anything to subvert your constitutionally protected rights." If you would like to counter this little patriotic ploy, fight fire with fire. Show up for the test wearing a little American flag lapel pin.

If your polygrapher is a prominent one, then you may expect to spend some time in an outer office before the pretest interview begins. While you are waiting, don't sit there and fidget or stare blindly into space. Why? Because that fancy office probably has a

one-way mirror disguised as a picture or even a fish tank. The polygrapher will be observing you from the moment you enter the office, looking for inadvertent signs of deceptiveness. Don't give him any. Keep yourself busy.

One of the best defenses is to bring something with you to read. More importantly, bring something to read that makes you look like someone to be treated with respect. Ask yourself, "Would I be more impressed if I saw a stranger in a waiting room reading Stephen Hawking's *A Brief History of Time* or a tabloid bearing the headline, "The Government Took My UFO Baby!" A local newspaper is always a good choice; *The Wall Street Journal* would be even better. Most current magazines would be all right (except for gossipy ones like *People* or *Us*). A professional journal or current bestseller would be better. No steamy romance novels, no potboilers, no pulp westerns, no tabloids, no comic books. And for God's sake, don't bring this book. You just want to have something with you to fill the time before your test begins. You don't really have to read what you bring, but you should go through the motions. (Remember, you're being watched.)

MEETING THE EXAMINER

Attitude is the key. Don't greet the examiner with a sarcastic remark like, "So, you're gonna try to read my mind, huh?" Your initial contact should exude friendliness. A firm (not vicelike) handshake coupled with a sincere and confident personal introduction will go a long way. I know it sounds corny to say you never get a second chance to make a first impression, but it's true. Psychologists know about the benefits of favorable first impressions, and you should too.

The "halo effect" refers to the tendency of individuals to allow their general initial impressions of

others to distort their overall judgments about them. This effect has been gauged in a number of experimental settings, and the results have been fairly uniform. In a typical university study, college students watched one of two videotapes of a college instructor. In one, the instructor acted in a warm and friendly manner. In the other, he appeared cold and aloof. After watching one of the two tapes, the students were asked to rate the examiner on friendliness, physical appearance, mannerisms, and accent (he was Belgian). As expected, the warm versus the cold variables affected the subjects' responses significantly. Those who had seen the instructor behave in a warm manner reported liking him much more than those who had seen him behave in a cold fashion. Of greater interest was the amount of "spillover" from these global reactions to his individual traits. Students who had seen him behave in a cold manner and who formed a negative impression of him also rated his mannerisms, appearance, and accent as unfavorable, and vice versa.

After completing their ratings, some students were asked whether the instructor's friendliness had affected their ratings of his appearance, mannerisms, and accent. Surprisingly, the students overwhelmingly rejected this idea. But when other students were asked whether they felt the instructor's appearance, mannerisms, and accent had affected their overall ratings of his friendliness, a number of them said yes.

These findings suggest that the students' view of the process was totally reversed. Clearly, they were unaware of the influence the halo effect had on them. The halo effect can result from anything that produces a positive or negative impression. A person can be regarded favorably because of being an outstanding athlete, a great scholar, a powerful business executive, a warm family member, or purely because he or she is physically attractive. The tendency is to perceive all of

a person's characteristics as favorable so that they are consistent with the initial overall impression. Unfortunately, the reverse is also true. For example, it is common to perceive an overweight person or one who is of an unpopular race or nationality as having other negative characteristics as well.

With this in mind, you should certainly greet the polygraph examiner in a friendly manner in the hope this will generate nothing but positive thoughts in his mind. This process continues as he leads you into the examination area, sits you down, and prepares to begin the technical portion of the pretest interview. During this time, the two of you will probably discuss the weather, sports, or other nonthreatening subjects. Remember, the examiner not only wants you to relax, he also wants you to dispel any negative feelings you may have toward him. He realizes his is not a popular profession and that many people think he is a bully or a monster. By setting a relaxed and easy tone at the outset, he wants to manipulate your attitudes and get you in the proper mind-set.

THE PRETEST INTERVIEW

Technically, the pretest interview begins when the examiner first meets you. It is a process during which each party sizes up the other. Some prominent polygraphers have stated that the pretest interview is *the* most important part of the whole procedure. Basically, its purpose is twofold: 1) to provide you with information about the examination and inform you of your legal rights, and 2) to persuade you that the examination is conducted professionally and that any attempts at deception will be painfully obvious. At this point, guilty suspects are supposed to recognize the confidence in the examiner's voice and start to get anxious. Innocent suspects, on the other hand, are

supposed to trust in the examiner's display of confidence and be less anxious.

The pretest also allows the examiner to assess any special conditions or circumstances that may affect physiological responsiveness. You should therefore expect questions about medical problems as well as drugs you may be taking that could influence autonomic responding (obviously, you should not mention drugs you may have ingested for countermeasure purposes). Although it is highly unlikely that an examiner will ask you to submit a blood sample, you might have to give a urine sample. Not to worry, though. Most urine testing labs will only screen for illegal drugs (e.g., marijuana, cocaine, heroin, etc.), so there is a good possibility that the ataractics described in the previous chapter won't show up.

If, however, you are unfortunate enough to have your sample sent to a really good lab and the ataractics are detected, there is no need to panic. All of the drugs outlined earlier are antihypertensives, so you could say that you were taking them for high blood pressure. If anyone asks you why you didn't tell the polygrapher about this medication, you can say that you had stopped taking the drug before the exam, and anything found in your sample must have just been a residual amount.

Once the small talk and pleasantries are over with and all the prerequisite information has been obtained, the examiner will get down to the real nuts and bolts of the pretest interview: convincing you of the polygraph's validity and formulating his questions. These two processes go on simultaneously. He will sound very confident and authoritative and will probably have well-rehearsed answers for the most commonly asked questions:

1. How accurate is the machine?
2. I hear these things are not conclusive.

3. Can't you beat these machines pretty easily?

4. Why should I trust that machine to make such an important determination?

5. Why do I have to take this test? I didn't do anything wrong.

6. What's the point in taking this test if it won't even hold up in court?

I wouldn't advise you to get into an argument with the examiner over any of these questions. If you get into a protracted debate with him, you will lose all that good will you have been trying to build. I recommend that you play the role he wants you to play during the pretest interview. Ask some questions, but don't be too skeptical. Unless you're a hermit, you have heard about polygraph exams from friends, coworkers, newspapers, or television. The polygrapher expects this. In fact, he wants you to ask questions about the procedure so he can gauge how much you know about the machine and how you feel about the process.

The trick here is to ask questions about polygraphs without sounding like a smartass or a know-it-all. There is a wrong way and a right way to ask a question. "Aren't these machines really pretty easy to beat?" is an example of the wrong way. First of all, this implies that polygraph exams aren't trustworthy and that polygraph examiners aren't capable of catching people who cheat. In only eight short words, you have managed to trash the man, his chosen occupation, and the industry as a whole. This is not the way to stay on his good side. Secondly, and perhaps more importantly, this question implies deception. The examiner may come right back at you with, "The only people I know who have to 'beat' a test are those who really have something to hide. Do you fall into that category?" Don't get caught in this trap! Think before you speak!

A much better form of this question would be,

"Someone told me about tricks you can use to make sure that you pass one of these, but they really don't work, do they?" You are making the same point, but you have softened it so the examiner will not feel you are challenging his authority. More importantly, by asking the examiner to confirm your "doubts" about countermeasures, you have shown him you are willing to bow down to the superiority of the machine. Polygraphers love a question like this because it implies that you think polygraph examinations really work, and it allows them to boost their egos by confirming your suspicions with a bunch of pseudotechnical jargon.

Pump the examiner up. Flatter him. But don't go too far. It can backfire if you start to gush all over him. Stay away from compliments about his clothes or overall appearance—they always sound phony. If you really want to stroke him, comment on his diplomas and certificates. Say something like, "I didn't know polygraphy took so much training. It must have taken you a long time to earn (always say 'earn'—never 'get') all of these." Done correctly, this phrase should imply a genuine admiration for your examiner's commitment to his profession. Another good ego booster is to pretend you've heard of the polygraph school named on his diploma. Say something like, "That's supposed to be a pretty good school, isn't it? I had a friend who was talking about going there." This demonstrates that you have respect for his profession (you can enjoy the quiet irony of lying through your teeth later).

Don't act like you are "above" this sort of thing. Once again, you run into the problem of downgrading the examiner's profession. You may believe (as I do) that polygraph exams are nothing more than electronic voodoo—a simplistic attempt to rectify such complex problems as employee turnover, theft, and drug abuse without spending the money to get the job done right.

Most polygraphers, however, are sincere in their belief that they provide a valuable service. You should not, therefore, walk into the examining room with a bad attitude. You may very well feel hurt or embarrassed or even outraged that you have to submit to such a test, but keep it to yourself. The fragile relationship you have developed with the examiner will stay on a friendly course if you can convince him that you, too, are dismayed at all the dishonesty in the workplace and realize that polygraph exams have become a necessary tool for weeding out thieves. Simply put, if he thinks you respect his profession, he may be more apt to give you the benefit of the doubt should your chart data fall right on the borderline between deceptiveness and nondeceptiveness.

It's very important to express confidence that you'll pass the test. As the pretest interview draws to a close, the examiner will have mentally labeled you as a skeptic or a believer, a troublemaker or a team player. Polygraphers frown on skeptics but enjoy the psychological control they feel they exert over believers. Naturally, you want to be seen as a believer. Get enthusiastic about the test and let the examiner know that you have absolute confidence in his abilities. Express a positive attitude that the exam will prove your innocence once and for all. By exhibiting this attitude, you are confirming to the examiner that he has done his job well—all your questions have been answered, all doubts cleared up. In his eyes, you have become the ideal examinee.

The typical ending to the pretest interview (which can last from twenty to ninety minutes or longer) consists of a final review of the test questions and a request that you sign a consent form. By this time, you should have a firm idea of which questions are controls and which ones are relevant, and the examiner should have them all listed on paper. If he doesn't show you

this list of questions voluntarily, ask to see it. If he hesitates, complain (gently) that you want to make sure that there are no unfair or improper questions. Almost all professional examiners will allow you to look at the list, but don't expect to find a big heading labeled RELEVANTS and a big heading labeled CONTROLS. You will have to pick those out yourself.

Fortunately, it is against the polygraph industry's rules to ask any question that does not come from this list. Therefore, once you have familiarized yourself with the controls and relevants on the page, you won't have to fear some kind of surprise question pulled out of nowhere. That kind of trick is really frowned upon by the industry and can be used as grounds for invalidating the whole test.

Once these details are cleared up, the examiner will ask you to give your voluntary consent to be tested. Consent procedures vary depending on the nature of the interview, the most important differences being between tests given for criminal investigations and tests given for preemployment screening.

If the exam is conducted as part of a criminal investigation, you should be read a copy of your Miranda rights and then be told that the exam is completely voluntary. You should also be informed whether or not the examination will be observed from outside the room or recorded or videotaped. Normally, all these specifications are typed up and you are asked to sign at the bottom. Applicants for employment need not be advised of their right to speak with an attorney but may, depending on local laws, be advised that the test is voluntary. In the case of such employment-related tests, along with a provision concerning voluntary consent, you should be told how the results of the examination will be used. For example, you may be informed that a copy of the test results will be provided to the sponsor of the exam (i.e., your prospective employer), that you have

a right to obtain a personal copy of the test results, and that you will not be asked any questions regarding political or religious affiliations, union activities, or sexual activities unless these areas are specifically related to the issue under investigation.

Treat cautiously any statement or paragraph that may seem to limit your legal rights. Some consent forms contain a section that protects the test sponsor or the polygrapher (or both) from liability. If yours has such a statement and you sign it, you may be waiving your rights to any future legal action. You should *never* sign a consent form like this unless and until you see a lawyer. Undoubtedly, the polygrapher will accuse you of overreacting or trying to hide something, but don't let him trick you. The only reason he wants you to sign such a statement is to keep from being sued! Believe it or not, polygraphers are being sued successfully by an increasing number of disgruntled individuals whose polygraph test results have had an adverse impact on their lives. Like doctors, polygraphers are having to purchase malpractice insurance. So don't let some smooth-talking polygrapher goad you into signing a waiver of your rights. He's not looking out for you; he's looking out for himself.

TESTING

So far, you have presented a charming, friendly, pleasant, flattering, and ingratiating personality. Now, however, you need to focus on the task at hand: beating the test. The actual polygraph test is relatively brief, and each examiner probably conducts his test in a slightly different way. But the general order of events is as follows.

Hooking Up

If you are not seated there already, the polygrapher

will place you in the examination chair. It will most likely be placed alongside the examiner's desk so that when you are seated he will be looking at your profile (or the back of your head) and you will be looking, most likely, at a wall. The polygraph machine and its attachments will be lying on top of the desk. First, the pneumograph tube will be placed around your chest. Some examiners will use two tubes and will place one around your chest and one around your stomach. Second, electrodes will be attached to your fingertips (in some cases electrode jelly will be applied to your fingertips to increase conductivity). Third, the sphygmomanometer will be placed around your arm and inflated slightly so that the machine can get a good cardio reading.

Ideally, this entire process should take less than a minute. Believe me, it can seem like a long minute. All polygraphers know that this hooking up process is a great fear inducer, and they will be paying particular attention to anything you say or do while the attachments are made. Therefore, don't get cute and make offhand remarks like "electric chair," "I'm in the hot seat now," "How soon till blast-off," or "Have you heard from the governor?" While it is a natural human reaction to make jokes in times of stress, the polygrapher may interpret them as indications of your guilt. The best thing to do is sit quietly and try to relax. If you are lucky, the examiner will give a running explanation of what each attachment is used for as it is applied. If he doesn't, ask questions. Concentrate on his words. Continue to exude an air of anxious optimism. That way you aren't just sitting there stewing.

The Stim Test: The Ultimate Deception

After you are hooked up, the examiner will begin recording physiological baseline measurements. Don't

be alarmed if these initial tracings look pretty damaging. This is natural and is called an "orienting response." Basically, an orienting response can be thought of as a natural tendency to show elevated responsiveness to any new stimulus. When referring to a polygraph exam, the orienting response is that initial anxiety you feel over actually being hooked up and having your autonomic responses recorded. This will subside eventually, and the examiner will watch the charts to get a clear indication of your normal level of arousal. When he is satisfied that he has enough baseline readings, he will most likely carry out what is known in the business as a stimulation or "stim" test.

Stim tests are designed to show even the most skeptical person that the polygraph machine can really differentiate between the truth and deception. It starts innocently enough: the examiner will ask you to pick a standard playing card from a group of cards or to choose a card from a special pack of numbered cards. In one version, the examiner will ask you not to reveal what the card (or the number) is, but to simply concentrate on it. He will then ask you a series of questions so as to determine what card or number was selected. This line of questioning will go something like, "Was it a spade? Was it a face card? Was it a black card? Was it the King of Spades?" Rest assured, he will be able to tell you which card you selected. What he will not reveal to you is that you have been conned. The deck of cards he used was probably marked, or the cards may have been laid out on the table in such a way that he can tell what card you selected simply from its position in the deck. Either way, he knew what card you selected even before you did.

The whole rigmarole of asking you questions about your card is what magicians call misdirection: a deliberate attempt to direct your attention away from how the trick is really done. Is this deception really

necessary? Well, yes and no. Actually, the polygrapher could figure out what card you selected without cheating, but that method is unreliable. Studies have shown that, based entirely on polygraph tracings, experienced examiners can correctly identify the chosen card up to 73 percent of the time. That figure, however, is not good enough for a polygraph test. Since the object of the stim test is to convince the subject that the polygraph can determine when deception is occurring, being correct only one-half to three-quarters of the time is not good enough. The need to be accurate 100 percent of the time requires examiners to cheat.

An alternate form of the stim test does not involve outright cheating by the examiner, but trickery is still involved. In this version, the examiner will ask you to pick a number from 1 to 10 and write it down where you can both see it. Next, he will instruct you to say "no" to each question of the form, "Did you write down number _____?" He will say that this is a procedure used to calibrate the machine so that he will have a clear indication of what your tracings look like when you tell the truth as opposed to when you lie. This statement is, of course, untrue and misleading, but the examiner will no doubt make a big production out of tearing the chart from the machine, showing you your tracings, and pointing out where you were lying.

Lots of people get taken in by these theatrics, and studies have shown that "successfully administered" stim tests can increase the validity of the polygraph exam (Senese, *Journal of Police Science and Administration*, 1976). If you know in advance that the polygrapher will be playing these little mind games with you, you will not be as likely to give the examiner credit when none is deserved.

The Real Test

After impressing you with his magic tricks during

the stim test, the examiner is ready to proceed with the real thing. The test will begin with a fifteen- to twenty-second (or longer) pause to allow your responses to return to baseline levels. A fifteen- to twenty-second pause will also follow each question, allowing time for the previous response to fade and the physiological measures to return to baseline. This procedure is followed throughout the test, with the examiner carefully noting on the chart when the test began, when questions were asked, and when the test ended. Any extraneous behaviors such as coughing, sneezing, or shifting positions in the chair are also noted. After the entire set of questions is asked, that particular test ends, and the examiner will usually deflate the blood pressure cuff so as not to cause you any undue physical discomfort. He may then ask for clarifications on certain questions or make other refinements, and then he will repeat the test two or three more times to give the examiner three to four charts from which he will render his opinion.

Don't be surprised if the examiner is called away from the room during testing. This is another common trick—to make you sweat it out alone with your thoughts and let your anxiety build. You should also expect this room to be equipped with one-way mirrors or listening devices (remember the consent form you signed?), so watch yourself. Don't fidget, don't try to look at your chart, and don't start talking to yourself. It is best to act nonchalant or even bored, and if you brought your reading material in with you, by all means, start reading. This will indicate to the examiner that you are not afraid of the test and have nothing to hide.

The Post-Test Interrogation

The final component of the examination is the post-test interrogation. If you're lucky, you may not have to go through this part of the process. If, up to this

point, the examiner believes you are being truthful, and if this view seems to be confirmed by a lack of strong physiological reaction to the relevant questions, then the final interrogation may be dispensed with. The polygrapher will tell you that he could find no indications of deception on your part and that he will say as much when he makes his report to the test sponsor. Consider yourself lucky—you have just passed your polygraph exam.

If, on the other hand, the polygrapher thinks you are being deceptive, then you have another ordeal to endure—the post-test interrogation. The examiner will remove the polygraph attachments, seat himself facing you—toe-to-toe, knee-to-knee, and face-to-face—and make an opening remark like, “I think you’ve got a problem.” For many polygraphers, the post-test interrogation and the confession it often induces is the object of the whole examination. Some long-time polygraphers even admit that they don’t care whether the test is valid or not; they only go through the process so they will have enough ammunition to elicit (coerce?) a confession during the interrogation.

Many researchers, including Lykken (1981) and Budiansky (1984), believe this is one of the most dangerous aspects of a polygraph exam because a naive suspect who is judged deceptive could be tricked or bullied into making a false confession. You should *never* confess to *anything* during the post-test interrogation or, for that matter, at any other time before, during, or after the test. If you confess, the polygrapher has won. He has earned his pay. You, on the other hand, have admitted your guilt and solved everyone’s problems. Remember, the results of a polygraph exam are not proof of anything. Even if you fail the test with flying colors, what has that proved? If you ask me, it only proves that you suffered from a lot of anxiety during the examination and didn’t respond

the way that this "professional" thought you should. In my mind, there is still a great amount of doubt that you are guilty of the incident under investigation. But when you confess, you remove all doubt.

If you really are guilty and you confess, you have let the box beat you. If, however, you are innocent and make a false confession, you will go through the rest of your life with a black stain against your name that should never have been there in the first place. And if you make a false confession and later try to recant, you will be labeled untrustworthy or unreliable, and people will have a hard time believing anything you say. Don't make the polygrapher's job easy! If he judges you deceptive, make him prove it. One study showed that an astounding 90 percent of job seekers who were rejected after being examined were tripped up not by their test results but by inadvertent admissions made during the post-test interrogation. *Never confess!*

A good interrogator will use a number of ploys to elicit a confession. He may become your "friend" and try to help you justify whatever it was you did so that it will be easier for you to "tell the truth." He will tell you that lying is difficult and tiring; telling the truth will bring about a great feeling of relief as you get the awful secret off your chest. He will try to get you to view him as a confidant, someone who really has your best interests at heart. Punishment will not be discussed initially; he just wants you to "set things right with your life."

If he senses any resistance on your part, he will move on to the next stage. He will tell you that your story doesn't square with the facts—it's just too incredible. He may try to trick you by claiming to have inside information or contradictory evidence provided by "other witnesses"; many times the witnesses and evidence are both nonexistent. Your denials and protests are cut off with a raised hand and a disappointed nod of the head. To

him, your denials are all transparent and futile.

He will try to make you believe that your sole objective is to convince *him* of your innocence. He'll tell you that his opinion carries the greater weight and that if you refuse to cooperate "the game is lost." As Lykken (1981) put it, "He wants to prevent you from stubbornly repeating the same story, 'take it or leave it,' because once you have ceased to care whether he believes you, then his leverage is lost."

Don't be intimidated. Don't listen to him when he says something like, "Well just look at the charts! We got these charts from you . . . they're just your body telling us what you are too afraid to admit . . . and they're saying that you're lying!" If he tries to get away with a statement like this, you should tell him that those charts don't "say" anything. They're just a bunch of squiggly lines.

If the post-test interrogation has disintegrated to this point, there is really no more reason to stay. Unless he is a police officer and you are under arrest, he cannot prevent you from leaving. Tell him that the conversation has obviously reached an impasse that is not likely to be resolved under the present circumstances and that you are going to leave. As you make your exit, he will most likely try to trick you into staying by commenting that "deceptive persons often remove themselves from an unpleasant situation rather than face it." Don't fall for this old line. The polygrapher knows he has lost you and is just grabbing at straws.

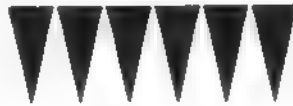
Before you leave the office you may want to ask him if there are any provisions on his report for you to make your own statement. If there are, then you may want to say something about the questionable validity of polygraph examinations. I've included a statement that you can cut out and take with you for just such a purpose (see Appendix C). Most likely, however, you

will not be allowed to make a statement on his report. You should still ask for a copy—a very reasonable request—and, if you want to rattle his cage a little bit, ask him for the name of his attorney. There is nothing like the implied threat of legal action to make someone think twice about crossing your path.



CHAPTER SEVEN

BEYOND THE POLYGRAPH: OTHER ABUSES



*"... He that hath
eyes to see and ears
to hear may
convince himself
that no mortal can
keep a secret. If his
lips are silent, he
chatters with his
fingertips; betrayal
oozes out of him at
every pore."*

—Sigmund Freud,
1905

*"Some people may
see the tests as an
improvement over
the lie detector, but I
see them as
psychological
rubber-hose
treatments
employers use to
intimidate people."*

—Michael Tiner,
legislative consultant
and member of an
OTA panel studying
paper-and-pencil
integrity tests

When the Polygraph Protection Act took effect in December 1988, many civil libertarians breathed a sigh of relief. With a single stroke of a pen, Ronald Reagan had greatly limited the extent to which private employers could invade the privacy of workers. Unfortunately, many employers felt lost without their good friend Mr. Polygraph, so they immediately set their sights on other ways to gauge the trustworthiness of both their prospective and present employees. Fortunately for them, entrepreneurs and quick-buck artists popped out of the woodwork selling all kinds of programs, equipment, courses, tapes, and seminars designed to help save the poor, victimized employer from his treacherous, thieving employees.

Today, there are no fewer than six techniques to choose from as management consultants make a

fortune filling the void left by the polygraph. Not surprisingly, these new methods invite the same criticisms that plagued the polygraph: invasion of privacy and lack of validity. If you are looking for a job or plan to look for one in the future, you stand a good chance of running into one of the following. Understanding what they are and how they work will give you a better chance at countering them.

KINESIOLOGY

Though actually misnomers, kinesiology and kinesic interviewing are the popular names for an examiner's attempt to judge your "true" character by interpreting telltale body movements and speech patterns. Practitioners of this art claim that the vast majority of people will give away deception through nonverbal cues even though they are successful in lying verbally. This is known as nonverbal leakage: true emotions are said to "leak out" no matter how hard the speaker tries to conceal them. A college student, for example, may say she is not nervous about a test but will bite her lower lip and blink more than usual—actions that often indicate nervousness. A young man waiting for a job interview may attempt to appear calm and casual, but he will mindlessly cross and uncross his legs, straighten his tie, touch his face, and run his fingers through his hair. As a result, he will come across looking like a nervous wreck.

The concept of leakage implies that some channels of communication leak more than others because they are less controllable. This theory is supported by several studies that have found that the body is more likely to reveal deception than the face. Tone of voice is also less controllable than facial expressions, so it may leak as well. Unfortunately, kinesic interviewing is almost impossible to detect. After all, who can say

what a listener is really focusing on during a conversation? Perhaps that personnel director was really listening to your history of past accomplishments and future plans. On the other hand, perhaps he or she was only watching for discrepancies between your verbal message and your body message. Who knows? About the only way to defend against this type of lie detection is to know in advance what kinesic interviewers look for. The following list of eight major nonverbal categories should provide you with the information you need to plug up some of those pesky leaks.

Proximity

In general, the more friendly and intimate one person feels toward another, the closer he or she will stand when communicating. Friends stand closer than strangers, and people who want to seem friendly may also choose smaller distances. A good polygraph examiner will use proximity to his advantage. During the pretest interview and the test, he will maintain an appropriate distance; not being your friend, he will not try to crowd your personal space. However, if he believes your charts indicate deceptiveness, he will move in very close during the post-test interrogation. He knows that this sudden change in proximity will add to your anxiety, and he hopes that the additional pressure will finally force you to make a confession. Don't cave in. If he moves his chair close to yours, just lean back and try to act as though it does not bother you. He may be invading your personal space, but you can't let that cause you to lose self-control. If you lean back and act as if his invasion doesn't bother you, he will eventually move away and try something else.

Orientation

The angle at which you sit or stand in relation to

another person can vary from head-on to side-by-side. Although orientation can vary with different situations, different cultures, and different sexes, those who are in a cooperative situation or who are close friends tend to adopt a side-by-side position, whereas people in a bargaining position tend to choose head-on positions. A polygraph examiner will most likely confront you with a head-on position during the post-test interrogation. Your goal should be to mirror his orientation. You can still lean back in your chair while maintaining the head-on orientation, but don't shift your position in the chair so that you present the side of your body to the examiner. This is usually interpreted as an unconscious attempt at deception (i.e., you are using your body as a shield to protect against the examiner's "frontal attack").

Research has found that there are many ways a person can position his or her body to denote affiliation with others, as well as relative social status. One researcher, for example, has suggested that when people sit facing us directly or leaning in our direction and nod in agreement to what we say, we tend to interpret this to mean they like us. In contrast, we seem to interpret the following actions as signs that people do not like us: sitting so as to avoid facing us directly, leaning away from us, looking at the ceiling or floor while talking, and shaking the head in disagreement with what we are saying.

With respect to social status, it has been found that asymmetrical placement of the limbs, a sideways lean or reclining position, and relaxation of the hands or neck are behaviors that denote a higher-class communicator relating to a lower-class listener. The lower-class listener, by contrast, will usually adopt a rigid and uncomfortable (though dignified) posture. Think, for example, of a corporate CEO reclining in a leather desk chair and issuing orders to his staff. He is

relaxed and comfortable; they are probably standing at attention and focusing intently on every word.

Two postural cues that are interpreted by kinesic interviewers as signs of guilt or deception are leaning toward the door of the examination room and slumping in your chair. Both should be avoided. The first denotes a desire to remove yourself from the stressful surroundings; the second is thought to indicate a desire to curl up and protect yourself from any incoming stimuli.

Head Movements

Head movements, especially nods, most often function as reinforcers to speech. For example, if you are speaking and someone is nodding his or her head up and down, you will tend to interpret that as acknowledgment or approval and continue to speak. Very rapid nods, however, indicate that the listener wants you to finish up what you are saying so he or she can speak. The affirmative quality of a nod is often used in lie detection. Many people will, for example, respond with an exaggerated "No!" when confronted with an unpleasant accusation. The head will first tilt upward and then, when the word "no" is spoken, it will rapidly tilt down to (or just below) the original position. This is interpreted as an affirmative nod that contradicts the verbal "no" message. Deception is therefore inferred. Similarly, a person who slumps his head downward (a half nod?) while he says no or just after he says no is also seen as deceptive. The same holds true for people who say no and then look away.

Facial Expressions

The face is one of the most useful communication areas. During conversations, a listener will usually provide continuous commentary on the speech of another through facial expressions. At the same time, a speaker makes facial expressions that indicate whether

what is being said is supposed to be funny, important, serious, and so on. Although you might expect the face to be a reliable indicator of deception, that is not the case. Because we develop considerable control over our facial expressions as we mature, an examiner can never be sure whether an expression presented is inadvertent or ingeniously calculated. For example, some people smile when they tell a lie. Others maintain a placid expression. However, neither pupil size or perspiration can be controlled adequately when anxiety is present, so these weigh heavily in an examiner's opinion of your veracity. (It is rumored that Yasir Arafat is such a firm believer in pupil size as an indicator of deception that he never removes his sunglasses while conversing with others—even indoors.)

Despite studies showing the ineffectiveness of facial expressions for the successful detection of deception, kinesic interviewers have compiled a substantial list of "reliable" deception indicators, including: smiling nervously, shutting your eyes or looking away after a denial, flaring the nostrils, raising the eyebrows, tightening or pursing the lips, losing color in the face, denying an accusation with a look ("Who, me?"), or denying an accusation and looking intently at the examiner.

The study of gestures moved from the lab to the general public a long time ago. In recent years, many books have been published that practically guarantee that you can tell exactly what others are thinking or interpret what they are saying by observing their body movements. An open palm is said to imply an invitation; crossed legs are defensive, and so on. No one has come up with a reliable dictionary of gestures, however, because their meaning depends on such things as the context of the communication, the person making the gesture, the culture of the person, and probably a lot of other factors as well.

Be that as it may, supporters of applied kinesics have constructed voluminous lists of so-called deceptive gestures. In fact, just about any gesture you can think of has, at one time or another, been labeled an indicator of deception: crossing your legs, rubbing your legs, crossing your arms, touching or rubbing your nose or chin, touching or cleaning your glasses, grooming (wiping your nose, touching or playing with your hair, fidgeting with your shirt buttons, straightening your tie, winding your watch), pinching your nose, covering your nose or mouth with your hand, moving your hands about (especially as if to wave off statements), holding your chin, touching your lips, licking or smacking your lips, rubbing or scratching your head or neck, tapping your fingers or toes, bouncing or swinging your legs, gulping or complaining of a dry mouth, and, of course, grasping the arms of a chair so hard as to produce white knuckles.

Gazing

During a normal two-party conversation, people tend to look at each other for periods of one to ten seconds. If the conversation is unimportant or simply uninteresting, the participants may spend as much as 75 percent of the time not looking at each other, but at their surroundings. If, on the other hand, the conversation is important or interesting, the percentage of time spent looking away may drop to 25 percent. People look about twice as much when they are listening as when they are talking. Investigations of the gaze phenomena have shown that gazes serve four major functions: 1) regulating the flow of conversation, 2) monitoring feedback, 3) expressing emotions, and 4) communicating the nature of the interpersonal relationship.

At the very minimum, gaze indicates interest or

lack of it. For example, an otherwise casual conversation can become an expression of romantic interest if one of the speakers maintains steady eye contact. Conversely, avoiding or breaking the contact is usually a sign that the person is not interested. Indeed, when someone does not make eye contact during a conversation, we tend to interpret this as an indication that he or she is not really involved. No matter how attentively someone answers questions, nods at appropriate times, and carries on the conversation, the lack of eye contact means he or she is not really interested in what we are saying. But there are exceptions to this rule.

Someone who is conveying bad news or is saying something painful may avoid eye contact. Lack of eye contact can also mean that the person is frightened or shy. Likewise, when people have feelings they are embarrassed about, they usually do not like to be the focus of a direct gaze. Eye contact can also be interpreted as a threat.

There is conflicting information concerning how gazes will be interpreted from a lie detection perspective. Some say you should not try to stare too long at your examiner; others say breaking eye contact is more damaging. A frightened look characterized by continually darting your eyes about your surroundings is said to indicate guilt, as is blinking or being "shifty-eyed." Staring at the ceiling, staring at the floor, or looking "through" the examiner are also commonly characterized as indicating deception.

Paralanguage

Variations in speech qualities, distinct from the actual verbal content, are called paralanguage and can carry a great deal of meaning. Pitch, loudness, rhythm, inflections, and hesitations all convey important information. For some people, a pause may be for

emphasis, for others it may mean uncertainty. Higher pitch may mean excitement, distress, anger, fear, or surprise; a low pitch can convey pleasantness, boredom, or sadness. Loudness can mean anger, emphasis, or excitement; talking softly may make a listener think you are unsure, embarrassed, or shy. Interpreting these characteristics of language seems to be the newest rage in the lie detection industry.

Several studies have indicated that the pitch of the voice is higher when someone is lying. This difference is usually extremely small, but recently developed electronic voice analyzers are supposed to be able to measure these fluctuations and provide "accurate determinations" of truth or deception. There is also speculation that deceit can be uncovered by paying careful attention to the patterns of a person's speech. Some say that an individual who pauses for a long time before answering a question must be trying to deceive (this inference is even more likely to be made if we are already suspicious of a person's motives). Other speech patterns said to indicate deception are: using shorter sentences, making more speech errors, and replying with more nervous, less serious answers. Finally, people are thought to use words differently when they lie than when they tell the truth; they are thought to make factual statements less often, make vague, sweeping statements, or leave frequent gaps in their conversation so as to avoid "giving themselves away."

One researcher believes that deceptive language lacks spontaneity. He theorizes that when you talk normally and without stress, you tend to repeat words fairly often. But when you feel a need to be careful about a statement that may be self-incriminating, your phrasing changes. The number of different words you speak increases because you choose words you wouldn't normally use. Although this method has had three unique tests (a rape trial, a murder trial, and Richard

Nixon's "Checkers" speech), there is no hard evidence to indicate that it is a reliable lie detection method.

Human Lie Detectors

Is the leakage hypothesis correct? Does the body send out unmistakable cues that point to our deceptiveness? More importantly, can these signals be deciphered accurately by kinesic interviewers, personnel directors, or police officers? So far, the answers appear to be yes, yes, and no, respectively.

Studies have shown that liars do tend to send out a wide variety of clues to their deceit, but most observers do not use all of this information, and the information they do use is not used well. For one thing, most people tend to over-rely on the verbal content, which causes them to miss important information being conveyed through other channels.

Also, people have trouble distinguishing deception from general ambivalence. This was shown in a study having three groups of "senders." The first group truthfully described their positive (or negative) feelings about another person, the second group untruthfully described their positive (or negative) feelings, and the third group described their genuinely mixed feelings. When the study was completed, the researchers found that observers were not able to distinguish truthful messages about mixed feelings from deceptive messages about positive or negative feelings. These findings suggest that people may be able to distinguish true expressions of positive or negative feelings from everything else, but they are still not able to isolate deception itself without any further information—all they know is that the person does not sound wholeheartedly positive or negative.

"But wait a minute," says the lie detection industry. "This study was conducted in an artificial laboratory setting. Why don't you give lie detection a

chance in the real world?" Two researchers (Kraut & Poe, 1980) acknowledged this criticism and set out to conduct a scientific experiment to see if ordinary people are any good at detecting instances of lying in the real world.

Ordinary citizens were approached while waiting for an airline departure in Syracuse, New York, and asked to smuggle some contraband past an interview with a real U.S. Customs agent. Of the people who agreed to participate, half were asked to play the role of "smugglers" and half were asked to serve as an "innocent" control group. The smugglers were given contraband, such as small pouches of white powder or miniature cameras, and were told to hide the items somewhere on their person. They were also told that a \$100 prize would be given to anyone who could make it past the customs inspector without being detected. The innocent group, by contrast, did not get any contraband to smuggle. Hidden video cameras were set up to capture all the smuggler/inspector interactions. The researchers were looking for nonverbal behaviors exhibited by the smugglers and the innocents as they were interviewed by the customs agents.

After all the encounters were filmed, the tapes were given to a group of judges whose task was to chronicle all nonverbal behavior they saw. Many of the nonverbal behaviors outlined above were noticed, including speech peculiarities, defensive orientations and postures, nervous gestures, strained facial expressions, and avoidance of prolonged eye contact. Once all the nonverbal behaviors were categorized, the tapes were shown to a second group of judges who had to decide whether each individual was a smuggler or not.

The findings? Surprisingly, both the smugglers and the innocents behaved in practically the same way, which may explain why none of the smugglers were detained by a customs inspector. Even more surprising

was the fact that none of the members of the second panel of judges could consistently spot a smuggler—and they knew in advance that at least some of the people on the videotapes had to be smugglers! What does this say about the leakage hypothesis? Interestingly enough, the experiment did lend some support to the notion that we constantly leak information. You see, despite the fact that none of the judges could accurately detect a smuggler, they were all fairly consistent when it came to describing the cues they thought were associated with deception. In short, this study showed that human beings are not very good lie detectors, either in the lab or in the real world.

We are, however, pretty good at describing how others ought to behave when they are lying, but what does that prove? Well, for one thing, it proves that this is an awfully poor technique to use if you want to try to determine someone's veracity. Nonverbal cues just don't supply us with enough information to make valid determinations of truth or deception; anyone doubting this should spend an evening with a master poker player. By the next morning, you undoubtedly will have learned the costly lesson that some people will appear more cool, calm, and confident when they're bluffing (lying) than when they're holding four aces.

PSYCHOLOGICAL STRESS EVALUATORS

Various methods of lie detection have been tested over the years to augment or even replace the standard polygraph examination. At present, researchers are developing lie detection techniques based on facial temperature, pupil and retina response, brain waves, and even stomach palpitations caused by rapid breathing under stress. Another method that once held promise dealt with body odor: apparently, we all give off a distinct body odor under stress. This was

abandoned when researchers realized that there were far too many body odors to classify accurately, and any distinctive odors that might be classified were easily adulterated by cologne or aftershave lotion.

The military has always been interested in new forms of interrogation and lie detection. This led two army intelligence officers to try to find the fastest and most efficient methods for detecting deception in captured prisoners. After examining the problem from several different angles, the officers hit upon a new approach: examine the characteristics of their voices. One of the officers, Lt. Col. Allan Bell, had learned that certain vibrations or "microtremors" in the voice change when a speaker is under stress. Bell decided that fluctuations in these microtremors could also alert an interrogator to possible deceptiveness, so he started designing a device sensitive enough to pick up and chart the inaudible fluctuations of these vibrations. He eventually recruited another intelligence officer, Lt. Col. Charles McQuiston, who also happened to be an army polygraph expert. Together, they left the service, founded Dektor Counterintelligence and Security, and started producing PSEs for use by the general public.

How the PSE Works

Like the polygraph, the PSE detects stress—not lying—by measuring certain psychophysiological responses in the person being questioned. While the polygraph records blood pressure, breathing, and skin conductivity, the PSE measures only the "buzzing" vibrations, or microtremors, that are part of the characteristics of a person's voice. With a tape recorder, an individual's voice is converted into electrical energy and fed into an electronic processor. The processor isolates the microtremors from the other sounds of the voice and measures the changes in electrical energy that occur during stress. A digital display converts the

electrical measure of the microtremors into numerical values, and a stylus charts the fluctuations on a bar graph. The bar graph is then analyzed for so-called deceptive patterns, and the examiner classifies the individual under investigation as either deceptive or nondeceptive.

Proponents of the PSE point out a variety of advantages: it's simpler, quicker to operate, and less threatening than a polygraph because it doesn't need any wires connected to the body. What's more, it can be used covertly. Job interviews, theft interrogations, or any telephone conversation can be recorded and later run through the machine without the subject's knowledge. Naturally, critics point out that the technique is flawed, has dubious reliability and validity, and unfairly invades the privacy of individuals whose telephone conversations are surreptitiously recorded and then analyzed without their knowledge or consent.

Anecdotal Evidence

Because the vast majority of rigorously controlled scientific studies give the PSE miserable performance ratings, its proponents often rely on unsubstantiated anecdotal evidence to impress prospective buyers of the machine. Some of these "case studies" are, if nothing else, interesting examples of the PSE in action.

* A free-lance writer used one to check tapes of Lee Harvey Oswald's statements after his capture in Dallas ("I didn't shoot anybody, no sir," Oswald said) and concluded that he was innocent.

* Other investigators checked out Edward Kennedy's televised remarks after the tragedy at Chappaquidick and reported that he, too, seemed to be telling the truth.

* John Dean, Howard Hughes, Patty Hearst, and

Richard Nixon have all had various statements evaluated for their truthfulness with a PSE machine.

- * The makers of the PSE have even used it to test contestants on the old TV game show, "To Tell the Truth," and claimed a suspiciously high 95-percent accuracy in spotting the liars.

- * According to the August 15, 1978 issue of *National Enquirer*, three U.S. Air Force officers who flatly denied that the United States was involved in some kind of UFO cover-up were actually lying. PSE evaluations of their recorded interviews were conducted by none other than Charles McQuiston himself.

- * McQuiston also reported in the October 24, 1978 issue of *National Enquirer* that "something extraordinary" happened to Carl Higdon, who claims he was abducted by a flying saucer and carried off to its native planet before being returned to Earth. According to McQuiston, "Some parts of his statements show stress, but other parts show no stress at all, indicating he's telling the truth."

- * Internationally known psychic Francie Steiger claims she is in daily contact with Kihief—her guardian angel. PSE examiner Forrest Erickson confirmed her statement in the October 24, 1978 issue of *Midnight/Globe*.

- * "Without a doubt [he] is telling the truth" was the statement made by Erickson on claims from another bizarre UFO case involving Mr. Charles Hickson. Hickson, you may remember, started a media frenzy in 1973 when he reported that he, along with a fellow shipyard worker, was abducted from a Pascagoula, Mississippi, swamp while fishing and given a physical examination aboard a UFO. (*UFO Report*, November, 1978.)

- * Erickson also gave his endorsement to the strange case of Travis Walton, a lumberjack who

claimed to have been "zapped" by a UFO, knocked unconscious, and carried aboard the vessel, where he subsequently regained consciousness and was surrounded by "strange-looking creatures." Walton's claims were further supported by McQuiston, who concluded that "there is little, if any, possibility of a hoax involvement in telling the story." (*Fate*, October, 1978.)

Controlled Studies of the PSE

Since the army had been inadvertently instrumental in the development of the PSE, you might expect that many federal agencies would be making great use of it. That, however, is not the case. Various military and other intelligence agencies did buy and test a few voice analyzers in the early 1970s, but most of those machines have been discarded, dismantled, or destroyed. The Pentagon's National Security Agency tested the device and found it "insufficiently reliable." The U.S. Air Force Office of Special Investigations conducted sixty tests of its own and ultimately declared that the PSE was "not useful." Finally, the army commissioned a comparative study of the voice analyzers and the polygraph at Fordham University and found that the PSE achieved an accuracy rate barely equal to that of pure chance. In other words, the government doesn't believe the PSE even meets the standards of the polygraph exam, and we all know by now how unreliable polygraph exams are.

The polygraph industry was quick to point out its displeasure with PSE technology. For reasons that may have had as much to do with protecting their favored "lie detection" status as with scientific rigor, the American Polygraph Association criticized the PSE on two fronts: 1) inadequate examiner training, and 2) inadequate measures of the various "information channels."

With regard to training, the American Polygraph

Association attacked the PSE companies for allowing their students to conduct real-life exams after only *five days* of training (even the brief training given to polygraph examiners in the private sector is longer than this). The PSE companies claim five days is long enough because their machines are simpler to operate than a polygraph (true), and the results are easier to interpret (debatable). As for the second criticism, the American Polygraph Association is squarely against using the PSE as a stand-alone lie detector because it measures only one physiological response (as opposed to the polygraph's three). In a conciliatory gesture, however, the APA went on to conclude that the PSE might serve as a possible aid to a standardized polygraph exam by gauging the stress associated with the verbalization channel, thus adding another bit of information to the evaluation.

The Real Test

Despite the bickering between polygraph examiners and PSE examiners, both sides privately agree that the real worth of these devices is in their ability to produce confessions. And just like a skilled polygrapher, a skilled PSE examiner armed with his charts can get many individuals to break down and confess. As I've said before, you should never confess to anything. Once you confess, you've admitted defeat; if you don't confess, then it's just your word against his.

With that in mind, here are some pointers, gleaned from a newsletter published by the International Society of Stress Analysts, on how to interrogate a theft suspect. (Keep in mind how you would respond to this treatment and whether or not you would be tempted to confess.)

- * Begin an interrogation immediately after determining that the charts point toward deception.

- * Confessions are elicited more easily when you are alone with the subject in a private room.

- * Don't show the charts to the subject unless his responses are "truly dramatic." Less dramatic patterns can lead to pointless arguments with the subject concerning your conclusions.

- * Don't bully your suspect; become his friend. Sympathize with him and tell him of others in the same situation who felt tremendous relief upon confessing.

- * Point out to the suspect any physiological indicators of deception he may be exhibiting in addition to his chart data (dry mouth, sweating, upset stomach, elevated blood pressure, red face, etc.).

- * Minimize the gravity of the crime to make it easier for the suspect to confess.

- * If your subject is nonemotional, appeal to his common sense. Point out the futility of lying.

- * Rationalize the offense by helping your subject blame others for the crime: justify his act, blame the victim, his accomplice, his wife, parents, partner, or anyone.

It's no wonder that this type of lie detection interrogation is often called the "psychological rubber hose."

PAPER-AND-PENCIL TESTS

Paper-and-pencil measures of honesty are quickly becoming the number-one method for preemployment screening. These so-called "integrity tests" were rarely used when it was still legal to administer polygraph examinations for preemployment screening, but they are now firmly embraced by business owners and personnel directors looking for an inexpensive (and still legal) way of weeding out undesirable job candidates. Integrity tests are based on the assumption that a more forgiving attitude toward dishonesty predisposes a

person to dishonest behavior.

These tests fall into two categories: overt honesty tests and broader-based personality tests. Overt honesty tests assess a person's attitude toward the problems of dishonesty in the workplace by asking, for example, for opinions about how honest or dishonest the average person is and how honest or dishonest the test taker sees himself as compared to the average person ("I believe that most people are generally honest," or "Compared to other people, I feel that I am fairly honest"). Broader-based personality tests, on the other hand, measure a broader range of traits, such as employee reliability, deviance, social conformity, loyalty, initiative, and hostility to rules.

Problems

The major flaw of these integrity tests is that in order to pass you must exhibit a punitive and authoritarian personality. If a test question asks, "Do you believe that an individual who takes a pen home from work is a thief," then you must answer "yes," because the test developers consider even these small crimes to be unacceptable. The rationale is that someone who commits or condones small crimes will progress to bigger and bigger crimes.

Another question might be: "The department store where you work has a strict policy of destroying all damaged merchandise so that they can collect the insurance for it. One day, a well-liked and reliable but financially struggling five-year employee is caught at a Dumpster removing disposable diapers from their damaged boxes so that he can take them home for his new baby girl. Should he be treated as a shoplifter?" Once again, if you want to pass this question, you have to answer "yes." The rationale is that a thief will be unlikely to recommend harsh punishment for acts he might commit himself, and he will probably also

contend that most people are just as dishonest as he is.

That may be true, but what about those people who are naturally lenient and are more likely to "give the guy a break"? Are they to be less trusted employees? Will they be less productive? Less reliable? And what about people who have a cynical nature—those who don't trust their fellow man and are always looking for ulterior motives? They may truly believe that most people take things from their employers, but if they respond affirmatively to this attitude on an integrity test, then they will be penalized for being honest! Is that fair?

A second problem with these tests is that they assume that thievery is a personality trait just as "outgoing, bubbly, and friendly" are. Consequently, you cannot admit to thefts in the past (like taking home a pen) because the test developers assume that if you have stolen in the past, you will steal again in the future. Of course, this is a totally unreasonable and unprovable hypothesis. In fact, recent research seems to indicate that employee theft is probably more dependent on situational factors (e.g., easy opportunity, resentment or anger toward employer, special need for the item) than enduring personality traits that can be measured by a test. In other words, past behavior is a poor predictor of future behavior, and if a company wants to reduce the amount of employee theft, it should spend its money on measures that will make it harder for an employee to steal rather than on some test developed to assess personality traits.

Other problems with integrity tests have to do with improper construction and, again, poor examiner training. In regard to the former, some psychologists or personnel directors simply go to an existing personality test, remove the sections that apply to social dysfunction or social pathology and then use this as an "honesty test." The problem with this practice is that the developer of the original personality inventory

never intended it to be pulled apart and used as some sort of half-baked honesty test—all his reliability and validity studies guaranteeing the usefulness of the test are rendered worthless when someone comes along and uses only the parts of the test that seem to measure a particular trait.

Secondly, these tests are often sold to organizations that have no one properly trained to administer, score, and interpret them. As any professional psychometrician (a psychologist who specializes in testing) will tell you, there is a big difference between administering and scoring a psychological test and administering and scoring a fourth-grade spelling test. Unfortunately, many companies don't realize (or don't care) that many variables must be controlled to get an accurate score on a psychological test. This may be one reason these integrity tests produce such a large number of false positives (those who are incorrectly labeled as dishonest). Studies have shown that 40 to 60 percent of all test takers fail.

Sample Test

Would you like to see how you might fare on an honesty test? Try the five questions below. Answer truthfully.

1) An employer discovers that a trusted, long-term employee has been taking home one or two dollars a week from the "coffee fund." Should the employer have him arrested?

Yes / No

2) How should an employee caught smoking marijuana on the job be handled?

Ignored / Warned / Suspended / Fired / Arrested

3) What percentage of your friends would you rate as really honest?

95% / 80% / 50% / 20% / 10% or less

4) What percentage of employees do you believe takes small things from employers from time to time?

95% / 80% / 50% / 20% / 10% or less

5) What percentage of people do you believe cheats on income taxes?

95% / 80% / 50% / 20% / 10% or less

How do you think you did? Well, if you answered "Yes," "Arrested," "95%," "10% or less," and "10% or less," you stand a good chance of passing one of these tests. If your answers were different, you may be in trouble. Remember, to pass a test like this you must never admit to *anything*. As Dr. Philip Ash, research director for the Reid organization explained: "Incredible as it may seem, applicants in significant numbers do admit to practically every crime in the books."

You must also remember to answer all the questions like an ultraconservative, extreme right-winger would: taking something (no matter how small) is always a crime, people who take things are criminals, and criminals should be arrested and locked up for as long as possible. Adopting this type of attitude is the safest way to pass a so-called integrity test.

GRAPHOLOGY

Graphology is one of the oldest and least convincing methods of lie detection used. It dates back hundreds of

years, with the actual term "graphology" having been coined by the French cleric Michon around 1871. Interest in graphological techniques has continued unabated in this century, and it is easy to go into any large bookstore and find half a dozen books claiming to possess all the secrets of handwriting analysis. There is even computer software now on the market that will produce a report detailing a person's "social behavior, intellectual style, personality traits, and physical, emotional, and material drives." All you do is key in the answers to sixty questions regarding a handwriting sample's characteristics. To help you along, the software includes twenty-eight handwriting samples so you can check up on such luminaries as Ronald Reagan, Elizabeth Taylor, Edgar Allan Poe, and Queen Elizabeth II.

Graphology as an employment tool initially developed its largest following in Europe, particularly France, where it is still practically impossible to be considered for a job unless you submit a sample of your handwriting for analysis. During the 1980s, graphology made its way into the U.S. business community, where today it is said to be used by five to ten thousand companies (although the numbers are difficult to substantiate because many companies, fearing ostracism by their competitors or clients, will not acknowledge that they rely on this hocus-pocus in making personnel decisions).

Now that the majority of preemployment polygraph exams are illegal, the reliance upon graphology is almost certain to increase. Some critics argue that these businesses are trading one form of witchcraft for another, but that hasn't stopped the International Graphoanalysis Society in Chicago from churning out more than ten thousand "accredited" graphoanalysts, with another two thousand on the way. Graduates of its correspondence course—the only one of its kind in the United States—earn the title "certified graphoanalyst" after eighteen months of study and "master graphoanalyst"

after thirty-six months. Upon completion of the coursework, these certified analysts are free to charge from thirty dollars to three hundred dollars per analysis, depending on the type of information the client desires.

What do graphoanalysts look for? Unfortunately, that is not a simple question to answer because there are several competing schools of graphology, each with its own history, approach, and theory. In fact, if you look through two or three books on the subject of handwriting analysis, you will notice there is little agreement on which factors are the most important. More disturbing is the fact that these books give totally different interpretations for the same factors.

Dozens of these so-called personality indicators may be analyzed (depending on which school you believe), but some of the most common ones are: size of writing; percentage of page used; slant of letters; height of letters; width of letters; relative consistency of slant, height, and width of letters throughout a sample; connectedness of letters within words; pressure on the page; spacing of words; regularity of crossed *t*'s and dotted *i*'s; where the *t*'s and *i*'s are crossed and dotted; and whether the letters loop above or below the line. Some analysts also measure the speed of a person's handwriting. How is an analysis of all these factors carried out? Once again, interpretations vary, but some of the possibilities include:

- * *Dotting i's and crossing t's.* Dots that look more like lines than dots are said to indicate anger. Dots to the left of the *i* show procrastination. Forgetting to dot the *i* shows inattentiveness, as does leaving the bar off the *t*. If the bar is above the *t*, the person is said to have high or "visionary" goals. The bar at the top of the *t* means the person has distant goals, the middle of the *t* means practical goals, and low on the *t* means low or no goals.

- * *Rounding m's and n's.* A rounded *m* or *n* is said to mean a person accumulates information and then makes

a decision. A more pointed *m* or *n*, one that looks like an inverted *v*, may indicate keen comprehension.

- * *Height of letter stems.* The farther into the "upper zone" the stems go, the more developed the imagination and creativity. Lower-zone stems indicate sensual perception, unconscious drives, and biological needs. Long *g* and *y* stems, for example, may show an unconscious but strong sense of materialism.

- * *Slant of letters.* Straight letters (depending on who you believe) are said to show objectivity or introvertedness. Letters that slant to the left show self-absorption, and letters that slant to the right show emotional sensitivity (or logic).

- * *Pressure.* Heavy pressure is said to indicate anger or stubbornness; light pressure denotes insecurity. Some critics of graphology suggest that you use a felt-tip pen when preparing your handwriting sample so that the "pressure" factor is rendered useless.

- * *Speed.* The speed with which you complete your sample is used by some analysts as a measure of how natural, spontaneous, and genuine you are.

- * *Consistency of height and slant.* A consistent pattern of letter height and slant is said to indicate balance and self-control in your life. Irregular patterns indicate that you are not in full control and that you let the events of your life overwhelm you.

At first glance, these interpretations, compiled from several books and a certified graphoanalyst, may seem silly. After all, does it really take eighteen months of training to interpret leaving the bar off the *t* as a sign of inattentiveness? I don't think so. But I also don't think that graphology should be brushed off as some sort of harmless parlor game. Consider the following.

The president of an Atlanta-area business dealing with photocopying equipment reported in the January 18, 1989 issue of *Atlanta Journal* that, based on a

graphoanalyst's advice, he has hired six good employees and screened out eighteen others with whom he was impressed initially. How do you think those eighteen people would feel if they knew they were screened out because a so-called expert didn't like the way they crossed their *t*'s and dotted their *i*'s? How would you feel? I would be mad as hell. But graphoanalysts will argue that they are trained professionals using tried-and-true scientific principles. Unfortunately for them, the mainstream scientific community does not agree, as the following sampling of conclusions from some controlled scientific studies of graphology demonstrates.

* Ben-Shakhar, Bar-Hillel, Bilin, and Flug (1986): "The graphologists did not perform significantly better than a chance model."

* Furnham and Gunter (1987): "... the theoretical basis of the method appears weak, nonexplicit, and nonparsimonious."

* Lester, McLaughlin, and Nosal (1977): "No evidence was found for the validity of the graphological signs."

* Rosenthal and Lines (1978): "Thus the results did not support the claim that the three handwriting measures were valid indices of extraversion."

* Vestewig, Santee, and Moss (1976): "It was concluded that the analyst could not accurately predict personality from handwriting."

Despite the negative findings, graphology continues to flourish because overworked, stressed-out managers are constantly under the gun to find reliable job candidates who won't rob the company blind. And since mainstream psychologists have yet to produce a simple and 100-percent predictive measure of personality, these managers feel forced to turn to the graphoanalysts.

Interestingly, most graphologists will not attempt to determine the sex of the writer from a handwriting

sample, even though the average American citizen has been shown to succeed in this task about 70 percent of the time. (To protect themselves from being brought up on discrimination charges, graphologists typically don't receive personal information, such as age or sex, about the applicant.) They explain their reluctance to predict sex by insisting that handwriting reveals psychological, not biological, characteristics. This sounds like a cop-out to me. I find it difficult to believe that these analysts cannot make a simple prediction of sex, even though they will not hesitate to make absolute predictions about such abstract constructs as a person's belief system, motives, and personality. Perhaps they don't want to make judgments about gender because it could too easily be used as a gauge of their abilities. After all, how much faith would you put in a three-page personality profile if the graphoanalyst couldn't even determine the sex of the applicant?

RECENT DEVELOPMENTS

One of the great things about the United States is that entrepreneurship is openly encouraged by the government through tax breaks, low-interest loans, and the like. Many times, the success or failure of a business depends not on the quality of the product, but rather on the product's ability to fill a need—often expressed as “being in the right place at the right time.” Such is the case with the lie detection industry. The banning of polygraph exams for most pre-employment screening left a void in the marketplace, and entrepreneurs have been quick to provide alternative methods of personnel selection that circumvent the Polygraph Protection Act.

The Quick Phone Test

Although Georgia-based TeleScreen was founded

long before the passage of the Polygraph Protection Act, the company realized a 100-percent increase in revenues in the two months prior to the ban on polygraph testing, and it expects to see increased revenues throughout the 1990s because this system can now be marketed as a legal alternative to the polygraph test. In TeleScreen's test, a job applicant telephones a computer and responds to 150 questions asked by a recorded voice. The applicant has only three seconds to respond to each question by pressing buttons for "yes," "no," or "not applicable." According to the test's creator, the quick response time prohibits the applicant from reviewing and possibly changing his answers (which a paper-and-pencil honesty test would allow) and thus promotes truthfulness.

At twelve to twenty dollars an interview, TeleScreen hopes to convince its prospective clients that it is both a legal and cost-effective alternative to standard polygraph testing. What's more, the duration of a TeleScreen interview is less than ten minutes, and the applicant doesn't have to be wired to a machine, making the procedure less stressful than a polygraph exam. On the negative side, there is absolutely no evidence that a quick response time automatically compels people to tell the truth. Also, applicants who take the test using a phone with touch keys mounted in the handset would have to listen to the question, remove the handset from his ear, find the right touch key, punch it in, and return the handset to his ear, all in the allotted three seconds. Needless to say, all this fumbling around could cause some applicants to be penalized unfairly.

Despite these drawbacks, TeleScreen aggressively markets not only its testing service, but also a stand-alone system you can purchase for your own place of business. The complete systems are priced from ten thousand to fifty thousand dollars. Add to this a four-

dollar software licensing fee for each interview once the system is installed. (These costs are, of course, deductible as business expenses.) As with many other forms of lie detection, it is difficult to establish an accurate estimate of its validity. Company accuracy claims of 95 percent are suspiciously high and should be taken with a grain of salt.

Brain Wave Analysis

This technique is scheduled to be on the market in 1992 and may already be in use in limited areas. Quite simply, it is purported to be a "polygraph of the mind." Instead of measuring the physical expressions of emotion—pulse rate, sweating, blood pressure, and breathing rate—it measures actual brain wave activity through electrodes attached to the scalp. These signals are then amplified and fed into a computer, which coordinates the information and displays it on a video screen.

The theory behind this technique is that normal brain wave activity will break into a special kind of trough called P3 wave whenever an individual is presented with sensory information that has a special meaning for him. University tests on students, for example, have used words like "cheating" or "cocaine" to see if they cause a shift into the P3 wave, the implication being that the students who exhibit such a shift might be involved in these particular activities. Obviously, this technique suffers from the same drawbacks as the standard polygraph. Most damaging is the assumption that any word possessing enough of the requisite "personal meaning" factor to cause a shift to the P3 wave automatically incriminates the person being tested.

Let's look at the word "cocaine," for example. Perhaps you exhibit P3 waves at this word because you grew up in a drug-infested neighborhood and barely survived all the turf wars and random acts of violence

associated with such areas. You may have never used cocaine in your life, but I would bet you that the word "cocaine" has a special meaning for you. Should you now be accused of using cocaine because you grew up in a bad neighborhood? I don't think so, and I don't think brain wave analysis has sufficient safeguards built in to protect you in such situations as these.

Brain wave lie detectors are still in the planning stages, and the basic system, if completed, is expected to cost ten times as much as a standard polygraph. The complexity of the system would also require much more training than is generally provided for the typical polygraph examiner. If past experience with the polygraph and psychological stress evaluator is any indication, however, I am afraid that someone will eventually come along and make the brain wave analyzer cheaper, lower the standards for training, and make a fortune. At the same time, thousands of people will be unfairly discriminated against simply because they didn't react according to some examiner's preconceived notion of normalcy.

CONCLUSION



What does the future hold for polygraph/integrity testing? I can foresee three possible scenarios:

1) An enlightened bureaucracy realizes the folly of veracity testing and quickly passes legislation to prevent it. (Not likely.)

2) An outraged public grows tired of lie detection abuses and forces Congress to act. (Again, not very likely.)

3) Things stay pretty much the same. (Very likely.)

It is a sad fact that we have become a nation of noncritical thinkers. By and large, we don't question the claims we read in the newspapers or see on TV because we assume they must be true. In short, we often choose to take things at face value when a little skepticism is in order. Consider the following, for example.

* Graphologists won't make judgments about the sex of a person based on a handwriting sample. Why not? I think it's a fair question, and one that should be answered before we let the graphologist delve into more abstract components of our personality.

* Polygraphers make the assumption that someone who lies must become physiologically aroused. Why? Where is their proof?

* Proponents of the Quick Phone Test assume that a three-second response time promotes truthfulness. Is it their claim that it takes more cognitive processing to lie than to tell the truth? Can they prove this?

Because we don't require the lie detection industry to answer tough questions like these, we have given tacit approval to its operations. I believe this has gone on long enough.

Unfortunately, the truth merchants have grown to the point that they now enjoy considerable financial and political clout. We may not be able to put them out of business, but we can certainly make their jobs more difficult. I hope that this book will help you to do just that.

Just remember, the outcome of an integrity test is very much determined by how well you perform under pressure. So good luck, and remember to practice, practice, practice.

APPENDIX A

POLYGRAPH DO'S AND DON'TS



IF YOU ARE ASKED TO TAKE A POLYGRAPH EXAM ...

DO learn your legal rights. As of this writing, at least eighteen states and the District of Columbia have statutes that either prohibit employers from requesting or requiring tests or forbid mandatory testing.

DO contact your union representative if you are covered by a labor contract. You may have some protection or recourse through grievance or arbitration procedures.

DO discuss the matter with fellow employees. On occasion, groups of workers have balked and their employers have backed down.

DO tell your employer that polygraph tests can be inaccurate and that the mainstream scientific community has serious concerns about their validity.

DO contact your local office of the American Civil Liberties Union (ACLU) or legal aid society. They can tell you what your legal rights are concerning polygraph testing.

DON'T be afraid to speak up for your rights.

DON'T expect to be treated fairly. Remember, polygraph examiners are paid to find the guilty—not to clear the innocent.

IF YOU AGREE TO TAKE THE EXAM . . .

DO study this book. You want to go into the exam with a thorough knowledge of what will go on inside that room.

DO practice identifying your question categories. You stand a much greater chance of failing if you can't differentiate between control questions and relevant questions.

DO practice your countermeasures. Practice makes perfect.

DO dress nicely for the test. If you show up looking like a bum, expect to be treated like a bum.

DO bring something to read. You never know who may be watching while you sit in the waiting room.

DO be on time! "Show up late, you've cast your fate."

DO be friendly. Make a good first impression.

DO express confidence that the test will clear you.

DON'T be sarcastic. Making fun of the examiner or the test itself will not score you any points.

DON'T be belligerent or argue with the examiner about polygraph validity. You want the examiner to believe that you are a willing and enthusiastic participant.

DON'T fidget. It makes you look guilty.

DON'T be shifty-eyed. That *really* makes you look guilty.

DON'T complain about a dry mouth. An examiner

will interpret this as fear over being found out and may press you even harder during the test or the post-test interrogation.

DON'T sign away any legal rights. An examiner will pressure you to do this, but don't cave in. He's just trying to protect himself, not you.

IF YOU THINK YOU'VE FAILED THE EXAM . . .

DO ask to see the test report. Also ask if you can make a statement on the report (see Appendix C).

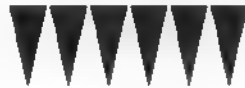
DO ask for a second opinion. This does not mean getting the examiner's colleague to reinterpret your present chart. This means going to an entirely different polygrapher and getting him to run a whole new test.

DON'T volunteer any information and **DON'T** admit to anything. One study showed that 90 percent of the job applicants who were rejected after being examined were tripped up by their own admissions, not by the test results.

DON'T be intimidated. If you're fired, harassed, or otherwise abused because of a lie detector test, see a lawyer. The American Polygraph Association and numerous authorities say that polygraph test results should never be the sole basis for termination.

APPENDIX B

POLYGRAPHERS' FAVORITE VERBAL PLOYS



Many polygraphers will use whatever means are necessary to get you to confess. One of their favorite tricks is to confuse you or misdirect your attention in an attempt to get you to see things their way. The following statements have all been used during actual polygraph examinations. Notice how they are designed to either set you up during a pretest interview or wear you down during a post-test interrogation. Following each statement is the thought process you must use to fight this kind of intimidation. Study these.

1) *"The machine says you're lying."* The machine says no such thing. It is just a bunch of squiggly lines. He's the one who is saying that I'm lying, and I don't put much faith in his opinions.

2) *"Remember, these exams*

are 95-percent accurate." Totally false. There has never been a properly controlled study resulting in accuracy rates that high.

3) *"I've been doing this a long time, and I know all the tricks."* He's putting me on the defensive and subtly warning me not to try anything. Don't believe this statement—studies have shown that even experienced examiners catch only the most blatant countermeasure attempts.

4) *"I'd stake my career on this machine."* Of course he would. Without it, he wouldn't have a career.

5) *"All the scientific evidence says that polygraph exams are reliable and valid."* A total falsehood. What the scientific evidence shows is that these exams are unpredictable at best, and I sure wouldn't want my fate trusted to one of them. If they are so reliable, why aren't they admissible in court?

6) *"I'm not out to get you."* Not true. The examiner is always trying to "get" someone, or he wouldn't be in business for very long. Remember, if he doesn't find someone guilty, he probably won't get any more business from that company or sponsor. Do you think he wants to risk that?

7) *"I'm a former police officer, and I've had _____ years of training and experience."* So what? The fact that he's a former police officer doesn't make him any more qualified to give polygraph exams than a former butcher, cab driver, or window washer.

8) *"If you're innocent, you've got nothing to worry about."* To prepare for this one, reread Chapter 2.

9) *"I can tell five minutes after I meet someone whether he is guilty or not."* The unmistakable sign of an arrogant examiner. If he's really that good, what does he need the machine for?

10) *"Countermeasures don't work."* Maybe he'd like to think so, but the truth is that there are

documented cases of people who have used countermeasures to beat an exam who have subsequently confessed or have been otherwise found guilty of the crime being investigated.

11) *"I'm going to have to tell your employer that you're the strongest candidate so far."* The ultimate in intimidation. The only reason he is sharing this opinion with me is because he wants me to confess. This is one of the oldest tricks in the book. Don't fall for it.

12) *"Remember, the machine doesn't lie" or "The machine never makes mistakes."* Of course it doesn't. It's just a machine that charts respiration, perspiration, and heart rate. He's the one I'm worried about making mistakes.

13) *"When you lie, you show definite signs of physiological arousal."* This has never been proven. When you're anxious, you show definite signs of physiological arousal, but being anxious and telling a lie are two entirely different things.

14) *"My interpretations are totally objective."* Like "military intelligence" and "jumbo shrimp," objective interpretation is an oxymoron. No human opinion can be totally objective, because the definition of objectivity requires that it be free of all personal bias or prejudice. Humans can only make subjective interpretations.

15) *"This test is for your benefit, not your harm."* What a joke. The test is for the employer's benefit, and the polygrapher usually doesn't care who gets harmed along the way.

16) *"I'll be watching for countermeasures, and I can almost always spot them."* Another statement designed to put me on the defensive. Think about this. How does he know he almost always spots countermeasures being used? Maybe he only spots the clumsy ones. The good ones, the ones that pass, may be slipping right by him. He has no way of knowing.

17) *"This machine can't be beat."* True, but an examiner can be beat.

18) *"We know you did it. Why don't you just confess and get it off your chest?"* Here, the examiner is trying to trick me into believing that he has some kind of inside information. This type of ploy works surprisingly often during post-test interrogations.

Do not fall for it.

19) *"Who are you trying to protect?"* This is one of those devious questions on the order of, "Do you still beat your wife?" There is no good way to answer it. If I answer that I'm not trying to protect anyone, the examiner will infer that I'm trying to protect myself. If, on the other hand, I admit that I am trying to protect someone, the examiner has won. He hasn't yet extracted a confession, but he's well on his way.

20) *"We could run this test one hundred more times, and I would still get the same results."* Time to ask to get a second opinion from another examiner. People who make statements like this have let their egos get the best of them. No one is able to reason with them because they think they're always right.

APPENDIX C

POLYGRAPH VALIDITY STATEMENTS



Office of Technology Assessment (OTA), an investigative arm of Congress, mandated to review and evaluate the advancements of and potential problems with current technology, has issued the following conclusions with respect to polygraph testing:

"... no overall measure or single statistic of polygraph validity can be established based on available scientific evidence. Further, regardless of whether polygraph testing is used in specific incident investigations or personnel screening, OTA concluded that polygraph accuracy may be affected by a number of factors: examiner training, orientation, and experience; examinee characteristics such as emotional stability and intelligence; and, in particular, the use of countermeasures and the willingness of

the examinee to be tested. In addition, the basic theory (or theories) of how the polygraph test actually works has been only minimally developed and researched.

In sum, OTA concluded that there is at present only limited scientific evidence for establishing the validity of polygraph testing. Even where the evidence seems to indicate that polygraph testing detects deceptive subjects better than chance (when using the control question technique in specific incident criminal investigations), significant error rates are possible, and examiner and examinee differences and the use of countermeasures may further affect validity."

CUT OUT AND SAVE!

GLOSSARY



anecdotal evidence: Uncontrolled and unsystematic observations. If you wear a particular shirt to a math test because you have always done well in the past while wearing it, you are basing your shirt choice on anecdotal evidence.

Backster school: A major polygraph training facility which teaches (among other things) that decisions of truth or deception must be made entirely on the data contained in the polygraph charts.

baseline: The readings on a polygraph chart that form a point of comparison for the physiological responses to the polygraph questions.

biofeedback: The control of internal processes such as heart rate, brain waves, or the galvanic skin response (GSR) through behavioral conditioning.

bogus pipeline: A procedure

whereby subjects are attached, via skin electrodes, to an imposing collection of electronic gadgetry so as to elicit truthful attitudes in situations where social desirability (i.e., subjects' desire to express socially acceptable opinions) may mask actual attitudes. The gadgetry is really junk, and the purpose of the procedure is to convince subjects that their actual attitudes are detectable.

construct validity: A type of validity determined by the extent to which the items making up a test are true measures of the construct or process being tested. In other words, the extent to which a test measures what it is supposed to measure.

control question: A type of polygraph question designed to be more arousing for nondeceptive subjects and less arousing for deceptive subjects than the relevant questions.

Control Question Technique (CQT): A polygraph testing technique that incorporates control questions.

countermeasures: Deliberate techniques used by subjects to avoid detection during a polygraph examination.

electrodermal response (EDR): A physiological measure that has been shown to be related to psychological arousal. It is measured as the electrical resistance of the skin through the use of electrodes attached to the fingertips.

false negative: An erroneous conclusion that an individual is not being deceptive when he or she actually is.

false positive: An erroneous conclusion that a person is being deceptive when he or she is actually being truthful.

field study: An experimental study using actual polygraph data from trained polygraph examiners.

galvanic skin response (GSR): See electrodermal response.

generalizability: The extent to which results of laboratory experiments can be applied to "real world" situations.

global scoring technique: A scoring procedure that uses behavioral symptoms, case facts, and other extraneous bits of information in conjunction with the actual polygraph chart data to make an overall determination of a subject's veracity.

Guilty Knowledge Technique (GKT): A polygraph testing technique that does not detect lying per se but attempts to detect whether a suspect has information about a crime that only a guilty person would have.

halo effect: The tendency to give individuals a rating or evaluation that is too high or too low overall on the basis of one outstanding trait.

hot question: A polygraph question that elicits a pronounced physiological response from a subject.

hypnosis: A sleeplike state induced artificially and characterized by greatly heightened suggestibility. Can be used as a cognitive countermeasure on a polygraph exam.

inconclusive: Outcome of an examination in which it cannot be determined from the subject's responses whether he or she is being deceptive.

irrelevant questions: Neutral questions designed to assess the subject's baseline physiological response to questioning and to provide a rest between relevant questions.

kinetic information: Gestures, expressive movements, posture, and tension patterns used in making judgments about persons.

laboratory study: An experiment conducted in a controlled environment in which the experimenter controls and manipulates all the experimental variables.

lie response: A presumed set of overt behaviors that are thought to be indicative of deception.

orienting response: An initial elevated response that occurs when a subject is presented with any new stimulus (for example, the first question on a polygraph exam will usually evoke an elevated orienting response).

paralanguage: Information conveyed by variations in speech other than actual words and syntax, such as pitch, loudness, hesitations, and so on.

physiological arousal: Responses related to increases in anxiety. Those measured in polygraph examinations include electrodermal response, blood pressure, and respiration rate.

pneumatic chair: A counter-countermeasure used by polygraphers to detect any extraneous physical movements that may indicate a physical countermeasure in use. It is usually a cushioned armchair fitted with strain gauges in the seat, arms, and back.

pneumographs: Rubber tubes placed around a subject's chest and abdomen to measure respiration.

post-test interrogation: The time period following the actual polygraph examination during which the examiner discusses the test with the subject and attempts to elicit a confession.

preemployment screening: The use of polygraph testing to assess the character of employee applicants.

pressure chair: See pneumatic chair.

pretest interview: The first portion of the polygraph testing procedure during which subjects are informed about the examination as well as their legal rights. In some pretest interviews, examiners also make observations about subjects' behavior to assist in their overall conclusions.

psychological separation: A presumed ability on the part of the subject to perceive relevant questions differently from "inclusive" control questions (that is, control questions whose content is of the same general nature as the crime under investigation).

Reid school: A major polygraph training facility that teaches (among other things) that conclusions of truth or deception should be based on behavioral symptoms, case facts, and other extraneous bits of information in addition to the data provided in the actual polygraph charts. This is known as a global scoring technique.

relevant questions: Polygraph questions about the topic or topics under investigation.

Relevant/Irrelevant Technique (R/I): A polygraph testing technique that utilizes two types of questions—relevant questions intended to assess a subject's degree of anxiety across a variety of subject areas and irrelevant (neutral) questions intended to assess the subject's baseline response.

reliability: The degree to which a test yields repeatable results. Also refers to the consistency with which similarly trained examiners give consistent scores to the same chart data.

sphygmomanometer: Blood pressure cuff used to assess heart rate.

stimulation test: A number or card test given to the subject before the actual test begins or after the first round of questions. Usually explained to the subject as a means of "calibrating" the machine; in reality, the stim test is designed to reassure truthful subjects of the machine's validity and provoke anxiety in deceptive subjects.

validity: A measure of the extent to which an observed situation reflects the "true" situation.

Countering **Hostile Surveillance**

**Detect, Evade, and
Neutralize Physical
Surveillance Threats**

ACM IV Security Services

PALADIN PRESS • BOULDER, COLORADO

CONTENTS

INTRODUCTION

PART I

Surveillance and Surveillance

Countermeasures Overview

Chapter 1

The Hostile Surveillance Threat

Chapter 2

Introduction to Surveillance

Countermeasures

PART II

Surveillance Operations Techniques

and Surveillance Countermeasures

Applications

Chapter 3

Surveillance Operations Overview

Chapter 4

Transition Stages

Chapter 5

Restrictive Terrain

PART III

Surveillance

Countermeasures Theory

Chapter 6

Surveillance Countermeasures

Principles

Chapter 7

Surveillance Countermeasures

Concepts

Chapter 8

The Chaos Theory of Surveillance

PART IV

Surveillance

Countermeasures

Applications: Manipulation

Chapter 9

Isolation Overview

Chapter 10

Isolation Methods

Chapter 11

The Break in Contact

PART V

Surveillance Countermeasures

Applications: Exploitation

Chapter 12

Introduction to Surveillance

Countermeasures Procedures

Chapter 13

The Multiple Sightings Surveillance

Detection Procedure

Chapter 14

The Temporary Break in Contact

Surveillance Detection Procedure

Chapter 15

The Break and Disappear

Antisurveillance Procedure

Chapter 16

The Temporary Break in Contact

Antisurveillance Procedure

For the people resemble a wild beast, which, normally fierce and accustomed to live in the woods, has been brought up, as it were, in a prison and in servitude, and having by accident got its liberty . . . easily become the prey of the first who seeks to incarcerate it again

—Machiavelli (circa 1515)

Physical Surveillance is the art of hiding in plain sight and stalking an unwitting prey

. Surveillance Countermeasures is the art of isolating the stalker and reducing the hunter to the hunted

—ACM IV (circa 2006)

The world around us is a dangerous and hostile one. Just as Machiavelli noted, ignorance of the evil makes for easy prey. We have entered an era with a level of prolific predators whom Machiavelli could never have fathomed, even as he penned those prophetic words. We will discuss the hostile threat in greater detail in Chapter 1, but in virtually all cases, the elements that threaten individual, corporate, or national security conduct surveillance operations either to further their objectives or as a primary means to an end.

In today's hazardous environment, security professionals must understand the threat and be able to advise clients regarding the appropriate countermeasures to protect against a hostile surveillance effort. Even the average citizen has security concerns and can benefit from gaining an understanding of the concepts of *surveillance countermeasures* that enhance personal protection.

Surveillance countermeasures are actions taken by an individual or security detail to identify the presence of surveillance, and if necessary, to elude or evade the individual or group conducting the surveillance.¹ In basic terms, surveillance countermeasures are actions taken to identify or evade a surveillance effort. Surveillance countermeasures consist of *surveillance detection* and *antisurveillance*. Although there are many categories of surveillance, this instructional manual focuses specifically on the detection and evasion of *physical surveillance*, which involves an individual or group of individuals moving by foot or vehicle in order to observe and monitor the movement of a target individual.

Over the years, ACM IV Security Services has discovered that the application of surveillance detection and antisurveillance measures is only marginally effective when the individual or security detail does not understand the theory, cause, and effect on which the measures are based. In fact, there is an infinite number of possible surveillance detection and antisurveillance maneuvers, but it is the underlying conceptual basis that makes them effective. The mere application of such techniques is amateurish by design if not planned and executed within the context of how surveillance countermeasures theory applies to surveillance practices. Unfortunately, in many cases, the rote practice of textbook methods without the full appreciation of the "art" and "science" of surveillance detection and antisurveillance measures can lead to costly—and even lethal—consequences.

This manual is unique in scope, as it is certainly not another basic reference on surveillance detection, countersurveillance, and antisurveillance.² Books and manuals abound with various tried and true methods and tactics to detect and evade hostile surveillance efforts. This manual is based on the assumption that the reader has an understanding of, or access to, this readily available information. What is not as readily available or intuitive to the security professional, however, is a reference on the art, science, and theory behind this key aspect of personal protection, given the wide range of potential threats. In fact, it is almost alarming that many security professionals and individuals who regard themselves as security experts are really masters only of the tactics, and not of the theory behind the tactics.

This manual details surveillance countermeasures concepts, techniques, and procedures that are proven effective against the spectrum of surveillance capabilities ranging from the very basic to the world's most sophisticated. This manual does not instruct to the "lowest common denominator," as most tactics focused publications do. Rather, this manual takes the opposite approach, as the practitioner who can apply techniques and procedures that can defeat the most capable adversaries can certainly defeat the lesser threats. The execution of *techniques* as components of a methodical *procedure* to effectively manipulate and exploit a hostile surveillance effort is representative of a security professional operating at the "Masters" level of surveillance countermeasures tradecraft.

UNDERSTANDING HOW THE SURVEILLANCE THREAT THINKS AND REACTS

This is the basis of effective surveillance countermeasures. The techniques and procedures presented in this manual represent concise applications of the most effective surveillance countermeasures based on a comprehensive analysis of hostile surveillance threats. Understanding how a surveillance effort will perceive and react to these countermeasures is vital to the effective application of specific surveillance countermeasures techniques. Individual surveillance detection and antisurveillance tactics are readily identified as such by a surveillance effort, and overcome. As opposed to a reliance on individual surveillance detection and antisurveillance tactics (maneuvers), this manual presents a process approach that enables systematic, discreet, and comprehensive applications for surveillance countermeasures methodologies.

Surveillance countermeasures applications must be conducted with an appreciation that the surveillance effort they are directed against has a strategy, is proficient, and can react and adapt based on the situation. Actions without perspective are tantamount to those of a chess player who jumps on the opportunity to take a knight with a pawn, without consideration of his opponent's strategy, intentions, and second- and third-order reactions.

Against an able opponent, it is likely that by opting for the immediate tactical success in seizing the knight, the player has contributed to a chain of events that will eventually lead to his demise in checkmate.

Chess analogies aside, the "mean streets" are not sterile environments, and even the most effective surveillance countermeasures tactics may be counterproductive if executed without a well-grounded appreciation of how a surveillance effort thinks and reacts.

Manipulate and Exploit

Manipulation and exploitation are at the heart of the surveillance countermeasures process. They require an understanding of how a surveillance effort thinks and reacts. An appreciation of how a surveillance effort will react to an isolated event is an important perspective, but it is a minimalist approach. The execution of effective surveillance countermeasures is a process. The ability to devise and execute effective surveillance countermeasures *procedures* requires an understanding of the overarching *principles* and *concepts* that translate into surveillance countermeasures tactics, techniques, and methodologies. The key point is that effective surveillance countermeasures procedures are comprised of tactics and techniques that constitute a methodical process. The integration of these common surveillance countermeasures tactics into techniques that *manipulate* and ultimately into procedures to *exploit* a surveillance effort represents the mark of a true professional.

Ingenious in Their Simplicity

This is how the true security professional should view the applications of advanced surveillance countermeasures principles, concepts, techniques, and procedures. Ironically, these sophisticated aspects of art and science are easily understood when they are broken down into their most basic elements. This manual presents intricate concepts in a methodical manner that truly does make them appear simple once broken into their components.

This manual is organized into five parts that must be studied in sequence in order to develop the incremental basis of understanding and to fully appreciate the principles and theory that translate to art, science, and execution. The information herein is presented in a technical and straightforward manner, as the intent is to inform and not to entertain. For this reason, the manual has been specifically designed as a concise reference manual for security professionals that can serve as a relevant framework for the development, training, and execution of security programs.

Reducing the Hunter to the Hunted

This concept is the essence of surveillance countermeasures. Every day and in all parts of the world, hostile surveillance efforts are stalking and exploiting unwitting prey. This manual demonstrates how the intended prey can employ expertise and ingenuity to detect, evade, and if necessary, completely assume the role of the predator in the neutralization of a hostile surveillance threat.

ENDNOTES

1. Surveillance countermeasures terminology is not always consistent among security agencies and professionals. The primary difference is that some use the term *countersurveillance* as synonymous with the term *surveillance countermeasures* used in this manual. Others use the term *countersurveillance* as synonymous with the term *antisurveillance* used in this manual. Although perhaps in a minority (since the term *countersurveillance* has a very specific meaning in the classical sense of espionage

and surveillance in which the firm is actively involved) ACM IV Security Services prefers to use the term *surveillance countermeasures* as the tactics, techniques, and procedures employed to counter the efforts of a hostile surveillance effort. The concepts and applications presented in this manual are consistent, regardless of the reader's preference in discipline terminology.

2. While this manual will address some specific tactical applications, these examples are provided within the context of applicable surveillance detection and anti-surveillance principles, concepts, techniques, and procedures. In fact, a detailed discussion of tactical applications would only serve to detract from the primary focus, which is the much more important aspects that enable true security professionals to understand the principles and concepts that drive the formulation and effective employment of tactical applications as part of a coherent process. The book *Surveillance Countermeasures* (ACM IV Security Services) is an excellent reference for specific surveillance countermeasures tactics and techniques.

Surveillance

and

Surveillance

Countermeasures

Overview

The Hostile Surveillance Threat

The new reality of the contemporary environment is characterized by a wide range of unconstrained threats that reflect the ever-growing and pervasive underworld of dangerous actors. The plethora of acute threats to the personal privacy and security of average citizens consist of common criminals and stalkers, private and corporate investigators, government-sponsored espionage agencies, and international crime and terrorist organizations.

In fact, the criminal enterprises that traffic in everything from drugs to human beings, and the terrorist organizations that recognize no bounds of conscience, epitomize the contemporary threats that do not acknowledge innocent bystanders and from whom no one is immune. As a disturbing omen, there is consensus among national security experts that the steady increase in threats to a wider range of individuals based on the disturbing trend of “pervasive insecurity” will continue well into the second quarter of the 21st century.

The spectrum of surveillance threats to personal security can range from surveillance operations with nonlethal intent to the most dangerous extreme operations conducted in preparation for some type of physical attack.

At the most basic level, criminals will case potential targets to develop information to maximize their probability of success in committing a crime. Although not generally associated with sophisticated surveillance efforts, another common threat to the personal security of many is the stalker threat, which involves surveillance of an individual for any number of reasons—none of which are in the best interests of the target individual. Less sophisticated criminal threats will also employ surveillance to develop information on potential victims for incriminating or exploitable purposes, such as blackmail or coercion.

Criminal, terrorist, espionage, and various other more sophisticated elements employ surveillance to develop information on individuals they intend to intimidate, exploit, or terminate. At the lower end of this threat spectrum, surveillance is employed to develop exploitable information in efforts to recruit or coerce unwitting individuals to provide information or other types of support. Even people with no readily exploitable attributes can be manipulated into compromising situations to develop the leverage necessary for coercion. At the higher end of the lethality spectrum, terrorists, assassins, and other murderous elements conduct comprehensive preoperational surveillance to maximize the probability of successful attacks. In preparation for criminal or terrorist acts, surveillance is employed either to monitor a target’s activity to determine where he is most vulnerable, or in preparation for the conduct of an actual attack.

Another factor that portends an enhanced threat across the spectrum is that the surveillance capabilities that were traditionally associated only with government-sponsored intelligence and security agencies have proliferated widely. Organizations such as criminal, terrorist, and corporate-sponsored elements now have the resources to conduct sophisticated surveillance operations that were previously associated with only the most capable governments. The fact that these elements have training

facilities and doctrinal manuals reflects a degree of sophistication that presents significant challenges to the community of security professionals

The duration of a surveillance operation depends largely on the sophistication and objectives of the surveillance effort. A surveillance effort to develop information on a target for purposes such as blackmail or coercion will normally be conducted in a more deliberate manner and will generally require more extensive coverage. A surveillance effort to determine when and where a target will be most vulnerable to attack will take relatively less time, because the surveillance effort will focus on key weaknesses rather than on the development of detailed evidence. And in the extreme, a very hasty surveillance effort may be conducted to find and fix the target just prior to an attack. Regardless of circumstances, the target cannot assume that there will be multiple opportunities to detect or evade surveillance, and should in turn exercise diligence at all times.

The objectives and importance of surveillance countermeasures are based on the logical and time-tested assumption that individuals conduct surveillance of a target only in order to do that individual harm. Although the existence of a surveillance effort will always imply some degree of harmful intent, it is the threat of physical harm that most vividly highlights the importance of surveillance countermeasures. Even a random or spontaneous act of crime is preceded by detectable indications. The effective identification of these indications could provide the time and opportunity to react in an evasive manner under life-or-death circumstances. In the case of the more deliberate and sophisticated physical threats such as terrorism, kidnapping, or assassination, the perpetrators will invariably conduct surveillance of the intended victim. In most cases, the surveillance efforts in preparation for these attacks can be readily detected, and in fact, post-event investigations of actual attacks regularly determine that there were detectable signs that the victims overlooked or disregarded due to a lack of security awareness.

SURVEILLANCE TERMINOLOGY

Surveillance is the systematic, discreet monitoring of an individual to develop information regarding his or her activities. Although there are many categories of surveillance—such as technical surveillance—this manual focuses specifically on the detection and evasion of *physical surveillance*. Physical surveillance involves an individual or group of individuals moving by foot or vehicle in order to observe and monitor the movement of a target individual. This is the most challenging and threatening form of surveillance in today's environment.

For purposes of clarity and brevity, the individual under surveillance is referred to as the *target*. The target will also be referred to generically as *he*. The term *target* can refer specifically to the individual, or if under the protection of a security element, the term may refer to the target individual and his security detail collectively. Many surveillance and surveillance countermeasures publications and training courses commonly refer to the target as the *principal*. This manual uses the term *target* because that is exactly what he is when in the crosshairs of a hostile surveillance effort. Despite this distinction, this manual will progressively detail methodologies to facilitate “reducing the hunter to the hunted.” In the final section, we will demonstrate how the target can rapidly transition status from that of a potential prey, to that of the predator.

The element conducting surveillance of the target will be referred to as the *surveillance effort*. A surveillance effort can range from one individual to a sophisticated operation consisting of numerous individuals with specialized vehicles, communications equipment, and other technical equipment. Although a surveillance effort can range from one to multiple personnel, the effort operates with a single focus and will therefore be referred to as *it* rather than "they."

The physical surveillance methods addressed in this manual are basically categorized as *vehicular surveillance* or *foot surveillance*. The term *surveillance asset* is used to refer to either a surveillance vehicle or foot surveillance operator. When the distinction between vehicle and foot is necessary, the surveillance asset will be specifically referred to as either a surveillance vehicle, or surveillance operator when on foot.

In order to be effective, a surveillance effort must physically observe the target's activities. For the purposes of this manual, when a surveillance effort is effectively following and observing the target, this will be referred to as maintaining *contact*. The term "in contact" is synonymous with "under observation."

SURVEILLANCE METHODOLOGY

A professional and effective surveillance effort is orchestrated in a systematic manner, employing tactics and techniques that best ensure discreet coverage of the target. These time-tested procedures are based largely on an understanding of how the average person observes his surroundings while walking or driving.

A surveillance operation will normally begin with limited information regarding the target's activities. As information is developed during the course of an operation, the surveillance effort will develop a pattern of the target's standard practices and routines that it will use to plan and conduct subsequent phases of the surveillance operation in a more secure and efficient manner. This process, referred to as *target pattern analysis*, is conducted to determine standard patterns of activity that can serve to effectively focus the surveillance effort.

A surveillance effort generally becomes more efficient and effective against a target after observing his actions over a period of time and becoming more familiar with his activities. This enables the surveillance effort to better anticipate the target's intentions and actions. This also enables the surveillance effort to determine the times and activities that are likely to satisfy the objectives of the surveillance, as opposed to those that are routine and insignificant. Target pattern analysis enables the surveillance effort to concentrate efforts on the times and events with the highest potential payoff, while limiting the amount of time that it is exposed to the target, risking potential detection or compromise.

The concept of target pattern analysis is a key consideration as it applies to the planning and execution of surveillance countermeasures. Generally, a surveillance effort will adjust its coverage based on how surveillance-conscious the target is observed or perceived to be. If the surveillance effort assumes that the target is not surveillance-conscious based on target pattern analysis and other information and observations, it will likely be less security-conscious in the employment of its tactics and the exposure of its assets. Conversely, if the surveillance effort suspects that the target may be surveillance-conscious, it will exercise greater operational security and will provide the target fewer opportunities for observation and detection.

A driving principle of surveillance is that most surveillance efforts will routinely break contact with a target rather than accept a high risk of exposure. Most surveillance efforts make operational security their highest priority, because if the target becomes aware of coverage, the surveillance effort is severely hindered or rendered completely ineffective. At the conceptual level, this is a key consideration as it applies to the planning and execution of surveillance countermeasures.

Introduction to Surveillance Countermeasures

Surveillance countermeasures consist of surveillance detection and antisurveillance. Although surveillance detection and antisurveillance have two different objectives, many principles and concepts apply equally to both. For the purposes of this manual, the term *surveillance countermeasures* is used when the concepts and applications being addressed apply to both surveillance detection and antisurveillance.

SURVEILLANCE DETECTION OVERVIEW

Surveillance detection consists of efforts taken to detect the presence of surveillance. Such measures consist of actions taken by the target (or a security detail escorting the target) to identify indications of, or to confirm the presence of, a surveillance effort.

Physical surveillance detection can be subcategorized as *passive* or *active*. *Counter-surveillance* is a more sophisticated and resource-intensive method of active surveillance detection. Although passive surveillance detection and countersurveillance are important surveillance countermeasures methods, this manual will focus primarily on active surveillance detection measures that are employed by the target, or a security detail escorting the target.

The principles of *observation* are key to surveillance countermeasures, particularly as they apply to surveillance detection. Surveillance is the act of *hiding in plain sight*. This is based on the understanding that the average individual would never suspect that the crippled homeless man, the loving couple, or the ice cream truck could possibly be surveillance assets. Surveillance professionals understand psychological factors such as perceptions and biases, and play on these factors as a form of applied science. The reality is that surveillance assets must maintain a range of vision with the target that is reciprocal. The art of hiding in plain sight lies in the fact that the target will invariably “see” surveillance assets during the course of an operation, but unless he is acutely surveillance-conscious, will not actually perceive them as such.

The effectiveness of all surveillance detection measures depends on the target's ability to observe his surroundings.

Surveillance detection maneuvers must factor in the ability to observe the desired reaction, because obviously even the best executed surveillance detection maneuver will be ineffective if the target cannot observe for the reaction of a possible surveillance effort.

One of the most effective methods of detecting a surveillance presence is to isolate surveillance assets for observation, retention, and subsequent recognition. However, this method of surveillance detection is time-consuming and assumes that there will be multiple opportunities to detect individual assets over time. This is not always a safe assumption, particularly against a more sophisticated surveillance effort that employs effective tactics, disguise techniques, and even rotates assets. Additionally, the time

required to conduct this deliberate method of surveillance detection is generally longer, and therefore assumes a less immediate threat, which is a risk that many targets and security details are unwilling or unable to accept. As a *procedure*, this method will be addressed in a later section, but not in intricate detail, because this manual is primarily focused on the more proactive and direct *techniques* that cut straight to the determination of whether or not a surveillance effort is present.

Passive Surveillance Detection

Passive surveillance detection consists of the target (or a security detail escorting the target) observing the surroundings to identify indications or instances of surveillance without taking any active measures. A general understanding of surveillance principles and tactics facilitates the effective application of passive physical surveillance detection. In fact, passive observation techniques serve as a basis for hostile surveillance threat awareness. Passive surveillance detection is conducted during the course of normal activities and is primarily based on an understanding of how a surveillance effort operates in order to identify activities or tactics that are indicative of surveillance. Passive detection is conducted in a manner that does not provide the surveillance effort, if present, with any indication that the target is observing for a surveillance presence.

Passive surveillance detection is most feasible when the risk of violent activity against the target is low, making the identification and neutralization of the surveillance threat, if present, less urgent.

Although passive surveillance detection is not usually effective in quickly identifying surveillance, it should always be employed in order to identify indications of surveillance that may justify the employment of more aggressive (active) surveillance detection techniques. In fact, personal security details continuously practice passive surveillance detection as a minimum baseline procedure.

Active Surveillance Detection

Active surveillance detection involves specific, usually preplanned maneuvers to elicit a conspicuous and detectable reaction from a surveillance effort, if one is present. As with passive detection, active surveillance detection is based on an understanding of how a surveillance effort operates. Such an understanding enables the target to employ active measures that will invoke compromising actions by the surveillance effort. In fact, active surveillance detection maneuvers are specifically designed to force surveillance assets to react in a manner that isolates them for detection. By orchestrating an unanticipated situation to which the surveillance effort must react, the target isolates one or more surveillance assets for detection. Active surveillance detection is employed when the target has identified specific indications of surveillance, or as a standard security practice prior to conducting private or protected activities.

The variations of surveillance detection tactics and techniques are virtually infinite, and essentially limited only by the imagination. Although a detailed explanation of surveillance detection maneuvers is beyond the scope of this manual, for perspective, typical examples consist of

- 1 Move into a turn lane or an exit ramp and then back into the general flow of traffic, observing for following vehicles that do the same
- 2 Cross over multiple lanes of traffic to make a turn or exit and observe for following vehicles that do the same
- 3 Drive into a highway exit, such as a rest stop, that enables the target to continue through without stopping, and reenter the highway while observing for following vehicles that do the same. Along city and other streets, there are many variations of this tactic that can be applied, such as through a strip mall or virtually any other parking lot that facilitates a smooth exit and reentry onto the main route
- 4 Cut through a parking lot to bypass a red light. This is also an effective antisurveillance measure against a security-conscious surveillance effort
- 5 Cul-de-sacs and dead-end streets are probably the most extreme types of restrictive terrain where surveillance assets may be induced into compromising situations by mirroring the target's actions
- 6 The 180-degree-turn (reversal of direction) is perhaps the most effective surveillance detection technique. Just as the name implies, this maneuver involves the target reversing direction and retracing the route just traveled. From the surveillance detection standpoint, the 180-degree-turn is intended to isolate potential surveillance assets and elicit a conspicuous reaction. This maneuver enables the target to observe for potential surveillance assets that are forced to bypass the target, to observe for potential assets that hastily and conspicuously move from the route to avoid bypassing the target, and to observe for potential assets that execute a 180-degree-turn where the target did, or at some other location along the route
- 7 The "blind turn" or other tactics employing the concept of a "blind spot" are essentially efforts to manipulate a surveillance effort into mirroring the target in a manner that makes it susceptible to surveillance detection. This concept will be addressed in some detail in Part V.

Countersurveillance

Countersurveillance differs significantly from other methods of physical surveillance detection in that it consists of actions taken by a third party (other than the target) to detect the presence of surveillance on the target. Countersurveillance allows the target to travel in a more natural manner, since he—or his security detail—does not have to concentrate on observing for surveillance coverage. Countersurveillance can be conducted by the target's security detail, but is not conducted by the security personnel who are escorting the target. Among the other key advantages is that

countersurveillance assets are able to position themselves in locations that will provide a field of observation that the target would not be able to achieve himself.

Although the focus of this manual is appropriately first-person surveillance countermeasures, countersurveillance is the most sophisticated and effective method of surveillance detection, and is practiced by many professional security, intelligence, and law enforcement agencies. In fact, intelligence operatives use countersurveillance to ensure that their agents are not compromised, and law enforcement agencies employ it to ensure the safety of their undercover operatives during dangerous operations.

Personal and executive security elements can employ the principles of countersurveillance to provide a layer of protection that is equal to that of the most elite agencies. The practice of sending a security detail ahead of the target to conduct forward route reconnaissance can be considered a form of countersurveillance, but this practice is most commonly conducted for the purposes of physical threat identification or neutralization.

Antisurveillance

Antisurveillance consists of actions taken to elude or evade an identified, suspected, or possible hostile surveillance effort. All antisurveillance measures are considered active, in that the target executes an active measure in order to elude or evade a surveillance effort. Although virtually all antisurveillance measures involve efforts to elude or evade, the most extreme antisurveillance objective—*neutralization*—will be specifically addressed in the final section of this manual. Otherwise, unless specifically noted as an application to neutralization, all other references to antisurveillance and surveillance countermeasures as they apply to antisurveillance involve the antisurveillance objectives of eluding and evading a surveillance effort.

Antisurveillance is employed as a standard security practice prior to conducting private or protected activities, or when the target has identified specific indications of surveillance and there is an immediate need to elude or evade. Since surveillance is always possible, antisurveillance can be employed even when there is no specific indication that surveillance is present. In fact, professionals in covert activities, such as espionage agents, invariably employ antisurveillance activities as a standard practice, due to their extreme need to ensure that their operational activities remain unobserved and undetected.

The number of tactical antisurveillance applications is virtually limitless and not within the scope of this manual, but some of the more common examples are turning or exiting a route at the last minute with no warning, or moving into a designated turn lane and then reentering the main flow of traffic at the last possible instance.

Although very overt and aggressive measures—illegal maneuvers that violate traffic laws—are among the most effective antisurveillance techniques. Running red lights, illegal left-hand turns, and illegal U-turns are among the most basic examples of antisurveillance techniques that gain their very effectiveness based on the fact that they are illegal. In many cases, not only will a surveillance effort—in order to maintain security—not continue to pursue the target after such an illegal maneuver, but depending on the nature of the element, they may not want to risk being pulled over by law enforcement for a violation. Covert or illegal elements conducting surveillance

cannot risk that type of exposure. A primary purpose of this manual, however, is to demonstrate that antisurveillance can be accomplished through sophisticated procedures that alleviate the need to carry out isolated, overt measures that will be readily identified as surveillance countermeasures.

As it applies to hostile threats, there is a distinction between antisurveillance and antipursuit. This manual addresses the techniques as they apply to the measures taken to elude a surveillance effort, or even to evade an aggressive effort that attempts to maintain contact despite active surveillance countermeasures. However, if and when a surveillance effort transitions into the attack phase of an operation, the target's efforts should transition as well from an antisurveillance to an antipursuit effort. This manual addresses the spectrum of antisurveillance techniques ranging to aggressive measures to evade determined surveillance efforts. However, antipursuit measures—such as defensive and evasive driving techniques—as they apply to the reaction to the threat of physical attack, are beyond the scope of this manual.

Surveillance

Operations

Techniques and

Surveillance

Countermeasures

Applications

Surveillance Operations Overview

INTRODUCTION

Although this section largely addresses surveillance operations, the specific aspects discussed apply to surveillance countermeasures. The intent, however, is not to provide a detailed reference on surveillance operations. Rather, the purpose is to provide a basic understanding of surveillance operational concepts and techniques as they apply to the examination of subsequent surveillance countermeasures issues. For this reason, it is important to note that essentially every point made here, and in the other two sections in Part II, is relevant to the concepts, techniques, and procedures that are built upon in Parts III, IV, and V. By discussing some details regarding surveillance countermeasures applications up front, the later sections are able to provide more concise explanations of the advanced surveillance countermeasure methodologies.

SURVEILLANCE IMPERATIVES: CONTACT AND MIRRORING

There are two overarching imperatives that any surveillance effort must adhere to in order to execute an effective physical surveillance operation: *maintaining contact* (observation) and *mirroring*. These two simple imperatives are the driving factors for the development and execution of surveillance countermeasures ranging from the most basic to the most sophisticated.

Maintain Contact (Observation)

A surveillance effort must maintain contact with the target through observation in order to ensure that the target is not lost and the surveillance can proceed effectively. Simply stated, if a surveillance effort is unable to maintain contact with the target, the objectives of that particular stage of the surveillance operation will not be achieved. *Although intuitively obvious, this simple fact is the driving concept behind the development and execution of the most effective surveillance countermeasures tactics, techniques, and procedures.*

Mirroring

In a general sense, a surveillance operation involves *mirroring* the actions of the target. Mirroring refers to the tendency of a surveillance effort and individual surveillance assets to duplicate the target's maneuvers. Obviously, it is the requirement to maintain contact that leads to the need to mirror the target's actions. As will be addressed, surveillance efforts with multiple assets will employ tactics that are specifically intended to minimize the level of mirroring, in order to enhance security. In fact, the more professional the surveillance effort, the more proficient it will be in employing surveillance techniques that enable it to discreetly maintain contact, while

maximizing the available cover to blend in with the surroundings and concealment to prevent detection. Regardless of degree of sophistication or number of assets, any surveillance effort must generally mirror the target's overall movements in order to maintain contact.

SURVEILLANCE STAGES

A comprehensive surveillance operation is a tactically complex effort, but for the purposes of this discussion, the dynamics of a physical mobile surveillance will be generalized into two basic stages: the *box* and the *follow*.

The Box

The box stage involves positioning surveillance assets to begin a mobile surveillance operation. This consists of positioning surveillance assets to begin the follow when the target emerges from a fixed location such as a residence or workplace, or when the target stops temporarily during the course of a mobile surveillance follow. The box is based on the systematic positioning of surveillance assets around the area where the static target is located in order to prepare for a mobile surveillance follow when the target begins to move. The techniques of the surveillance box basically consist of the logical coverage of roads or routes by which the target can depart the fixed location. In some cases and based on target pattern analysis, a box may be established around an area which the target may be anticipated to travel through, rather than around the target's known or suspected static location.

The Follow

Once the target begins to travel, the surveillance effort will transition to the follow stage, which involves the transition from static positions in the box stage to a mobile surveillance follow and continues throughout the mobile surveillance of the target while traveling by foot or vehicle. A standard surveillance operation will consist of a succession of transitions between the box and follow stages until the operation is terminated. A given phase of a comprehensive surveillance operation will normally terminate when the target reaches a terminal long-term stay location, such as a residence at night or workplace during the day. In the meantime, the surveillance effort will depart to "cool off" and then return to establish the box when target pattern analysis has indicated that the target can be expected to emerge from the location.

The Mobile Surveillance Follow

Most of a standard surveillance operation's time and effort will be spent during the actual follow phase. For this reason, it is during this phase that the target will have the opportunity to employ the widest range of surveillance countermeasures. The follow phase of a surveillance operation can be conducted either by vehicle or by foot. Obviously, the target's mode of travel will dictate the surveillance asset employed. For our purposes here, the tactics for the mobile surveillance follow will be addressed as they apply primarily to a vehicular surveillance. This is appropriate since most targets' travel is usually conducted by vehicle, and virtually all high-risk personnel

traveling under the protection of a security detachment will be restricted primarily to vehicular travel

Regardless of how many surveillance assets are employed in an operation, at any given time there will always be at least one asset that maintains observation (contact) of the target. Intermittent losses of contact based on anticipating the target's actions, temporary blind spots, and exchanges between assets are normal. However, a surveillance effort will avoid letting the target go unobserved through options that would allow the target multiple alternative routes of travel, unless the effort were confident of the target's destination based on target pattern analysis or other means.

During the course of a follow, the members of a surveillance effort with multiple assets will *hand off contact* with the target among each other. The most basic example of this *hand-off* process is when the target is traveling along a route and then takes a turn onto another road. In this case, the surveillance asset traveling most closely behind the target will continue straight at the intersection, while another surveillance asset that is further out of observation range will take the turn and establish contact (observation) with the target.

The surveillance follow should consist of a succession of handoffs in order to minimize the amount of time that a single asset is exposed to the target for observation and detection. This is also an effective method of disguising the fact that the surveillance effort is mirroring the target's movements. In virtually all cases, however, there is a varying degree of time—normally seconds—when no asset will have contact with the target as the hand-off is executed.

The *floating box* is a surveillance method that is characteristic of a more sophisticated surveillance effort, as it generally requires multiple assets and a voice communications capability between assets. This method requires a minimum of three assets but is most effectively employed with four or more. Just as the term implies, the floating box involves surveillance assets moving at a pace with the target while traveling along parallel routes for a more secure and effective reaction to a turn in either direction. Given the example of a standard city block in a vehicular surveillance, the floating box would consist of at least one asset traveling behind the target on the same road, while other surveillance vehicles travel along each of the two parallel roads.

A complete floating box formation would also include a *lead* asset, alternatively referred to as a *cheating* asset. In the example of the vehicular street surveillance, the lead vehicle will travel ahead of the target on the same route and can warn the surveillance effort of approaching hazards or options, and can be positioned ahead of the potential obstacles in case the following surveillance assets are held up. In some cases, the lead vehicle could be the asset responsible for contact (observation) with the target at a given time.

Whether surveillance assets travel by foot or vehicle, the terrain and traffic patterns will dictate their following distance. In open terrain, the surveillance effort will generally increase following distance due to the greater range of observation for both the surveillance effort and the target. In denser traffic, the surveillance effort will normally follow more closely to maintain observation and be in the appropriate position at critical points along the surveillance route—primarily at traffic options.

Any sophisticated surveillance effort operates based on an understanding of the principles of observation, and will conform to what should be perceived as the norm with respect to the surrounding environment. A surveillance effort must use *cover* and

concealment to protect its activities from observation by the target. The term *cover* here is used in the classic espionage and investigative sense of *cover* for action, which simply means blending in with the surroundings to appear normal. *Concealment* can consist of a number of possibilities to include physical barriers, but generally, in a surveillance operation the primary method of *cover* and *concealment* for surveillance vehicles is other vehicles, and the primary method for surveillance operators on foot is the surrounding pedestrian traffic.

The Mobile Surveillance Follow—Mirroring

The concept of mirroring warrants specific attention in regard to surveillance countermeasures as it applies to a mobile surveillance operation. In most surveillance operations, the mobile follow stage makes up the large majority of the operation. For this reason, it is primarily during this stage that the surveillance effort will have the most exposure to the target and will consequently be most vulnerable to surveillance detection. Although there are other opportunities to detect or elude surveillance, it is generally during the follow stage that the target will employ the most effective surveillance countermeasures techniques. Mirroring is a key aspect that the target will attempt to detect through passive observation and active detection measures.

The degree to which a surveillance effort can conceal instances of mirroring is primarily based on the degree of training, the number of assets, and the sophistication of the effort. In fact, surveillance efforts employ tactics such as hand-offs, the floating box, and lead assets specifically to minimize the degree of mirroring. As a general rule, the fewer the assets available to the surveillance effort, the more it will be required to directly mirror the target's movements in a manner that is susceptible to detection.

Regardless how many surveillance assets are employed in a given operation, at any time there will always be at least one asset that maintains observation (contact) of the target and will therefore generally travel at a pace similar to the target's in order to maintain a standard secure following distance. Mirroring is basically an effort to place a surveillance asset in a position that best enables maintaining *contact* and best positions the asset in anticipation of the target's next maneuver.

Normally, mirroring consists of the surveillance vehicle maintaining a standard speed and distance (pacing), and changing lanes or taking turns as the target does. At a very basic level, if the target is traveling on a road with two lanes in each direction and is in the left lane, the surveillance vehicle will tend to position itself in the left lane as well in anticipation of a possible left turn. Alternatively, there will be a tendency to follow in the right lane if this is the target's lane of travel.

Although this form of mirroring (also referred to as *silhouetting*) has its surveillance detection vulnerabilities, it is preferable to the alternative, which is to be out of position when the target takes a turn and have to conspicuously cut across traffic in order to maintain contact. Obviously, other factors—such as the amount of traffic and following distance—will impact positioning, as traveling in a different lane than the target does have some advantages in regard to observation and security. If this can be accomplished in a manner that enables the surveillance asset to react appropriately,

The Mobile Surveillance Follow—The Lost Contact Drill

During the course of a follow, the surveillance effort may lose sight (contact) of the target for any number of reasons. When this occurs, the surveillance effort will take the necessary measures to attempt to regain contact with the target before he reaches a traffic option that would provide multiple possible routes of travel (or escape). If the surveillance effort is unable to reestablish contact prior to the traffic option, it must initiate a *lost contact drill* in an attempt to regain contact. The lost contact drill is a standard surveillance technique that involves the systematic execution of a series of maneuvers to regain observation of the target. This basically involves the immediate prioritization of the target's likely routes of travel from the traffic option.

Even when the surveillance effort is confident of the target's route of travel, it will normally, as a standard precaution, send assets to search along alternative routes of travel to prevent losing the target completely and having to terminate the operation. The effectiveness of this technique is directly based on the number of assets available to search along the alternative routes. For example, if a surveillance effort is forced to initiate a lost contact drill at a standard intersection at which it is assumed that the target's most likely option was to continue straight, then the first asset to the intersection would continue straight in search of the target. The next asset to arrive at the intersection will take the second most likely alternative (left or right), and the third asset will turn to check down the remaining alternative route.

Obviously, in this example, if the surveillance effort is limited to one or two assets, then one or two possible routes of travel would not be searched, potentially limiting the effectiveness of the lost contact drill. If adequate assets are available, additional assets reaching the point of lost contact would reinforce along the possible routes in the same order of priority to provide additional search capability at traffic options further along the respective routes.

As will be addressed in the fifth and final part of this manual, the lost contact drill concept is a key component of the most effective surveillance detection and antisurveillance procedures.

Transition Stages

INTRODUCTION

Transition stages (points) present challenges to the surveillance effort from the standpoint of maintaining contact with the target while avoiding detection.

The primary transition points in a surveillance operation are when the target transitions from a static to mobile status and the surveillance effort transitions from a box to a follow, or when the target transitions from a mobile to a static position and the surveillance effort transitions from the follow to the box.

The transition stages of a surveillance operation present observable and exploitable profiles that can result in unique vulnerabilities to surveillance countermeasures. At the most basic level of observation and change detection, an observant target is better able to detect surveillance assets as they transition from a static to mobile status, or from mobile to static status. This, coupled with a basic understanding of how surveillance assets can be expected to position themselves to establish a box and subsequently initiate a follow, is key to detecting surveillance.

Although not transitions associated with the transitions of a surveillance phase, two other transition stages that may occur during the course of the follow are the transition from vehicular surveillance to foot surveillance, and viceversa.

These are also elements of the surveillance follow that present a multitude of surveillance countermeasures opportunities if properly exploited.

Transition Stages—Static to Mobile

The positioning of a surveillance effort for a box involves the logical positioning of surveillance assets to discreetly initiate the follow once the target either travels through or emerges from within the box area. Obviously, the number of surveillance assets available will dictate how the box is established. Depending on the number of assets available, the surveillance effort will prioritize positioning based on the target's most likely routes of departure or transit.

This prioritization process is a key concept because if there are not enough surveillance assets to cover all possible routes, then a corresponding number of routes will not be covered based on the assessment that the target is least likely to take these routes. If there is only one asset, that asset will need to be positioned in a location that will ensure that it can both observe the target when he begins to move and initiate the follow. If the number of surveillance assets available exceeds the number of routes, the surveillance effort may opt to employ a *trigger* asset to alert the effort that the target is moving, and to position other available assets sequentially along the possible routes of departure as reinforcements.

When the target begins to emerge from a location where a surveillance effort would establish a box, if present, he will observe for indications of surveillance. In most cases this will involve no active measures and will consist of passive surveillance detection.

Observation for change detection purposes is most effective in areas where the target is very familiar with the normal surroundings, such as the neighborhood he lives in. The target will initially observe for vehicles or individuals who are conspicuously placed to act as a potential trigger. Unusually placed trucks, vans, or vehicles with tinted windows are particular indicators. As the target begins to move, he will observe for individuals or vehicles that conspicuously transition from a static to a mobile status. When the target departs the potential box location by vehicle, he will observe for vehicles that are located in likely positions to pull out and assume the follow, focusing primarily on vehicles that pull out behind the target from parallel parking positions or from positions adjacent to the primary route, such as parking lots and side streets. Although the list below is not all-inclusive, when observing for possible surveillance vehicles parked along the route of travel or in adjacent areas, the target will specifically look for vehicles exhibiting some of the following indications of boxing surveillance vehicles:

1. Passengers in vehicles (perhaps even with seatbelts on)
2. Engine running and exhaust emanating
3. Brake light engaged
4. Windows clear in inclement weather
5. Interior vehicle lights on

Transition Stages—Mobile to Static

This transition involves the target stopping during the course of the follow. It is normally associated with a short-term stop, so in the case of vehicular surveillance, the surveillance effort would likely not transition to a foot surveillance to cover the target during the stop. Therefore, the primary objective for the surveillance effort is to establish a box in preparation for when the target begins to move again.

An example of this transition is when the target pulls into a gas station to refuel. This is a good example of a stop with an opportunity to observe surrounding traffic while conducting a plausible activity (refueling). Regardless of the stop location, it should provide a plausible reason for the stop (cover for action) and the opportunity to observe inconspicuously for surveillance assets.

During this transition, there is an inherent vulnerability to detection as the surveillance assets maneuver based on the target's actions and may be forced to pass directly by the target's position. This effort to establish a box hastily also presents a window of opportunity for antisurveillance if the target begins to move before the surveillance assets are established in their respective box positions.

Transition Stages—Vehicle to Foot

Unless the surveillance effort anticipates the transition from vehicular surveillance to foot surveillance and prepositions operators on the ground, this transition can be one of the most effective from the surveillance countermeasures perspective. In reaction to this transition, if the surveillance effort has sufficient assets, it will deploy foot operators to the ground and then establish a box with surveillance vehicles around the target vehicle location. Due to the nature of a foot surveillance,

with its own unique challenges, the transition from vehicle to foot surveillance is also one of the most effective for antisurveillance purposes

With a more sophisticated surveillance effort, vehicles may be employed to support the foot surveillance by ferrying operators ahead of the target and relaying communications. As another example, an operator in a stationary vehicle can read a map and give foot operators movement instructions or other information, such as possible hazards that the target and operators may be approaching

If the surveillance effort loses contact with the target during this transition, the surveillance effort is reduced to conducting random foot searches while waiting for the target to return to his vehicle. In this case, the surveillance effort has a means of reinitiating the surveillance when the target returns to his vehicle, but will not be aware of the target's activities while contact was lost. It is interesting to note that espionage operatives who are confident that surveillance is present will use this technique as a primary means of antisurveillance. By eluding surveillance, the operative is able to conduct his operational activity and then return to his vehicle, which is still under the observation of the surveillance effort.

For a sophisticated surveillance effort with multiple assets to operate by foot or vehicle, the foot-to-vehicle transition is standard and will cause no significant problems. Surveillance efforts with limited assets, however, will encounter significant challenges executing this transition in an effective manner. This will normally require that foot assets move at a faster pace as they anticipate the target's return to his vehicle. This sense of urgency to return to the surveillance vehicles and be in position to assume the vehicular follow presents a profile that is susceptible to surveillance detection. If the surveillance assets are unable to discreetly move faster than the target in returning to the vehicles, the transition presents a risk of lost contact that the target can exploit for surveillance countermeasures.

Restrictive Terrain

RESTRICTIVE TERRAIN INTRODUCTION

The terrain and other environmental factors dictate a large part of how a surveillance effort conducts its follow of the target. Canalized terrain, choke points, and traffic hazards are examples of restrictive terrain types that facilitate surveillance countermeasures. Given the requirement to maintain contact with the target, restrictive terrain will usually force the surveillance effort to assume additional risk of detection in order to ensure that observation of the target is maintained.

Restrictive terrain is employed to isolate potential surveillance assets for surveillance detection purposes, and also to conduct or to posture for the execution of surveillance detection and antisurveillance measures. The key enabling concept of restrictive terrain is that the target will force the surveillance effort into a situation that restricts its freedom of movement, making it vulnerable to surveillance countermeasures.

Although a significant enabler for surveillance countermeasures purposes, restrictive terrain is a true double-edged sword for the target who actually suspects surveillance, but does not know whether the intentions of the surveillance effort are lethal or nonlethal. This is a critical consideration when determining whether to employ these enablers, because in many cases the restrictive terrain that the target can exploit for surveillance countermeasures purposes would likely be the very same restrictive terrain that a hostile element would choose to execute an attack on the target, if that were the intent.

Traffic Hazards

Traffic hazards are areas along a route of travel that can force a surveillance effort to slow down or come to a halt, or areas that provide the target multiple options of travel. Generally, if the target enters a traffic hazard ahead of the surveillance effort, or when not under observation by the surveillance effort, the risk of losing the target is significantly increased. Common traffic hazards include intersections with traffic lights and areas of dense traffic. Such hazards can either cause the surveillance effort to move into close proximity with the target or to lose contact altogether. The surveillance countermeasures implications of traffic hazards are obvious, as they force the surveillance effort into a slow-moving or static position that may be readily observable by the target. Particularly when moving from a relatively open area into an area with traffic hazards, the surveillance effort will tend to push in close to the target to avoid losing contact. Traffic hazards support antisurveillance by serving as obstacles to the surveillance effort as well. For example, the target may be able to clear the traffic hazard and “break away” while the surveillance effort is held up.

A category of traffic hazard that requires additional consideration from the surveillance countermeasures standpoint is *traffic options*. Although very common, a location such as a street intersection that provides the target multiple options of

travel is a traffic hazard, because if the surveillance team does not have contact with the target when he passes through the option, the surveillance effort will be forced to initiate a lost contact drill, not knowing the target's direction of travel from the intersection. Although not necessarily restrictive in the physical sense, traffic options in general do restrict a surveillance effort's freedom of movement, as assets will normally be compelled to reduce following distance when approaching the options in anticipation of the target's possible turn or change of direction.

Choke Points

Choke points are terrain features that generally cause traffic to slow down and concentrate in density. Various examples of choke points include construction zones, toll roads and toll booths, and areas where high-traffic, multiple-lane roads merge into fewer lanes. Choke points provide a number of key enabling characteristics in regard to surveillance countermeasures. For surveillance detection purposes, *choke points* may cause a following surveillance effort to slow down and perhaps push in close to the target, facilitating observation and detection.

As they apply primarily to antisurveillance, choke points can provide a degree of separation between the target and the surveillance effort. For example, when the target, traveling ahead of the surveillance effort, clears the choke point, he will be able to break away from a following surveillance effort.

Canalized Terrain

Canalized terrain consists of areas where freedom of movement is restricted to one primary route. Examples of such terrain are stretches of highway, rural roads, road construction zones where entry and exit are restricted, and roadway bridges or footbridges. The key exploitable concept of canalized terrain is that it provides a surveillance effort with no secure parallel routes or the ability to discreetly turn off of the route once committed onto it. By vehicle, oneway streets provide another dimension to a canalized route that further limits mobility for a following surveillance effort.

For surveillance countermeasures purposes, the exploitation of *canalized terrain* negates the ability for the surveillance effort to execute a secure floating box follow, and forces the surveillance effort to commit all its assets along a single route behind the target. Inducing the entire surveillance effort onto a single canalized route enhances surveillance detection through observable factors such as "convoying," by fanning out at the end of the corridor, or through the execution surveillance detection tactics, the most effective (yet potentially overt) of which is the 180-degree turn or reversal of direction. The exploitation of canalized terrain combined with a traffic hazard, choke point, or other type of obstacle becomes an effective antisurveillance measure.

Intrusion Points

Intrusion points are locations with a single primary point of entry and exit. Basically stated, an intrusion point is a location that forces surveillance assets to either "intrude" upon the target in close proximity or break contact and await the target's

exit from the location. Common intrusion points are dead-end roads and cul-de-sacs by vehicle, and small street-side business establishments by foot.

As it applies to vehicular surveillance, dead-end roads and cul-de-sacs are the extreme in terms of *choke points* because they completely restrict movement once committed. Again, restrictive terrain such as *choke points* will also serve to isolate the target with the surveillance effort, making the target extremely vulnerable to attack if that were the intent of the surveillance effort, or if the effort feels that it must act based on being compromised ("fight-or-flight").

By foot, intrusion points can be selected that enable the target to observe for potential surveillance operators who choose not to enter but rather linger outside awaiting the target's exit. Intrusion points with a secondary exit, such as a back door to a business, can be exploited to elude a surveillance effort, but such tactics would be readily perceived as overt antisurveillance measures.

Open Terrain

Just as the term implies, *open terrain* consists of areas where there are no, or relatively few, physical obstacles to obstruct observation for either the target or surveillance effort. Open terrain is restrictive terrain from the standpoint that it negates cover and concealment, and therefore restricts freedom of movement.

By drawing a surveillance effort into an area where there is little vehicular or pedestrian cover and concealment, the target can better isolate and identify the surveillance effort. The obvious risk, however, is that if there is a danger of attack from the surveillance effort the target will have set himself up in a vulnerable position by allowing the effort to isolate him in a secluded area.

Open terrain forces a surveillance effort to make a trade-off between line-of-sight observation and how closely it chooses to maintain contact with the target. For instance, if the surveillance effort chooses close contact over distance, it makes itself immediately vulnerable to detection. Alternatively, the surveillance effort that chooses to distance itself for security purposes makes itself much more vulnerable to antisurveillance.

Restrictive Terrain—Foot Surveillance Applications

Surveillance countermeasures principles and techniques generally apply equally to vehicle and foot surveillance. Given this factor, this manual is primarily focused on surveillance countermeasures applicable to vehicular surveillance because this is how most potential targets will spend the majority of their travel time. Additionally, most targets who travel under the protection of security details will travel only by vehicle when there is even a remote risk of surveillance or attack.

In general, there are some basic noteworthy differentiations among foot and vehicular surveillance. By foot, the target does not have the range of vision that is afforded by a vehicle's mirrors for surveillance detection, making efforts to observe the surroundings for the presence of surveillance more difficult to conceal, if the target is in fact being observed. This makes it easier for a surveillance effort to identify surveillance detection when a target appears unusually observant of his surroundings.

Another disadvantage to foot travel is that it is generally less canalized. While vehicular surveillance is restricted to established roadways and thoroughfares, foot

surveillance affords more flexibility in travel, as foot surveillance operators can maneuver in many directions with equal speed and security. Another significant disadvantage to surveillance detection on foot is that if there is a risk of attack, the target is not afforded the protection provided by a vehicle, and in most cases, the ability to accelerate away from the threat is much more limited.

On foot, the target can use much the same methodology to exploit canalized terrain and choke points as with vehicular surveillance countermeasures. Canalized terrain may consist of any restricted walkway, street overpasses, bridges, and even elevators or escalators if employed with caution. Canalized terrain may offer the target traveling on foot a natural opportunity to facilitate rear observation, but normally it will be exploited through the incorporation of a 180-degree turn or a stop-and-turn.

Public locations such as department stores, malls, business complexes, and parks are among the places in a foot surveillance operation where operators are most vulnerable to detection. In many circumstances, public locations offer variations of restrictive terrain that provide among the best opportunities for surveillance detection and antisurveillance. In most cases, public locations will force surveillance operators much closer to the target than they would otherwise allow themselves to get.

The basic principles of surveillance in public places are similar to those of choke points and intrusion points, in that they force surveillance operators to concentrate and stagnate. The presence of restrictive boundaries and nonstandard terrain imposes unique constraints and vulnerabilities on surveillance operators. The nonstandard terrain works to the benefit of the target for surveillance detection purposes because it forces the surveillance effort to use special or modified tactics. In essence, public locations force a surveillance effort to rely more on adaptability and resourcefulness than on a standard systematic formula of tactics, rendering surveillance assets more vulnerable.

In most circumstances, people on foot are moving with a purpose or destination. Those who are not are easily isolated from the surrounding populace. This is another key aspect of public locations that can be exploited for surveillance detection purposes. When individuals go into a public location, such as a store, they do so with a purpose. When surveillance operators follow the target into a public location, they must immediately contrive a plausible and natural reason for being in the location (cover for action), leaving them immediately vulnerable to detection if they are not able to adapt. In fact, the target can choose public locations that effectively isolate surveillance operators who enter but are not prepared to adapt to the surroundings. Locations with a standard dress code or in which clientele may be expected to dress in a particular manner or undertake a unique activity are very suitable if employed properly.

It is always important to note that surveillance operators will avoid making eye contact with the target because when this occurs, the asset is considered "burned" and of no further use to the surveillance effort.

This phenomenon results in an almost instinctive or compulsive reflex in close quarters that is highly indicative of surveillance.

Surveillance

Countermeasures Theory

Surveillance Countermeasures Principles

INTRODUCTION

There are three general surveillance countermeasures principles that directly impact the application of surveillance countermeasures across the spectrum, particularly from the perspective of determining the best means to achieve the desired objectives. Not only are these principles important in the formulation and execution of surveillance countermeasures techniques, it is also vital that security professionals understand these principles, because they can be deceptive if taken out of context.

A detailed discussion of these principles is appropriate for any forum addressing surveillance countermeasures, but for the purposes of this manual, these principles reinforce the need for security professionals to take the application of surveillance countermeasures beyond the mere execution of tactics and techniques and advance to a more sophisticated procedural approach. By way of introduction, these three principles are:

1 Surveillance countermeasures principle: the more active, the more effective.

In general, the more active (overt or aggressive) the surveillance detection or antisurveillance maneuver, the more effective it will be in achieving the desired result.

2 Surveillance countermeasures principle: surveillance detection enables antisurveillance.

Active surveillance detection techniques can be effective antisurveillance techniques.

3 Surveillance countermeasures principle: antisurveillance enables surveillance detection. Antisurveillance techniques can also be very effective in achieving the objectives of surveillance detection.

While these principles are widely accepted among the community of professionals in many cases, they can focus the applications of surveillance countermeasures in the wrong direction if the broader implications are not fully understood. Key to this understanding is that these principles are focused on the execution and effectiveness of individual maneuvers and techniques. As this discussion will demonstrate, by focusing on the tactics rather than on a process, the target is reduced to executing techniques that must be more active or overt in order to be effective. This implies an increased risk that surveillance countermeasures will be identified by the surveillance effort as such, potentially leading to unintended and dangerous consequences.

SURVEILLANCE COUNTERMEASURES PRINCIPLE:

THE MORE ACTIVE, THE MORE EFFECTIVE

In general, the more active (overt or aggressive) the surveillance detection or antisurveillance maneuver, the more effective it will be in achieving the desired result.

The potentially misleading part of this principle is that it equates "effective" with "good." This can be misleading in the sense that even if a maneuver is effective in detecting or evading surveillance, if the overall process objective includes ensuring that the surveillance effort does not suspect surveillance countermeasures, then the maneuver is not effective in the broader sense. An appreciation of the *covert-overt spectrum* is necessary to understand that there are varying degrees of "effectiveness" based on the specific surveillance countermeasures objectives.

Active surveillance detection and antisurveillance measures are conducted along the range from *covert* to *overt*—hence the term the *covert-overt spectrum*. Covert surveillance countermeasures are executed discreetly and are intended to detect or elude a surveillance effort without being recognized as active countermeasures. Overt surveillance countermeasures are intended to detect or elude with less or no regard whether the surveillance effort detects them as such. In simple terms, the more covert the measure the less active it is, and the more overt the measure the more active it is.

Generally, the more covert or discreet the surveillance countermeasures technique, the less effective it will be in meeting immediate surveillance countermeasures goals. Conversely, the more overt or active the method the more effective it will be in meeting immediate surveillance countermeasures goals. Consequently, the more overt the method, the more identifiable it will be to a surveillance effort (if present) as surveillance countermeasures.

The covert-overt spectrum is based on the target's subjective professional judgment regarding the need to execute effective surveillance countermeasures versus the acceptable risk of being observed conducting active or overt measures by the surveillance effort, if present. The determination of where along the spectrum of covert to overt the surveillance countermeasure employed will fall is normally based on an assessment of the risk versus the need to positively confirm or elude surveillance activity. If, at a certain point in time, the benefit gained by executing a successful surveillance detection or antisurveillance maneuver does not outweigh the risk of demonstrating surveillance awareness to the surveillance effort, the target will weigh in favor of more covert techniques. Conversely, if ensuring the execution of a successful surveillance detection or antisurveillance method warrants the risk of an aggressive display of surveillance awareness, then the measure employed will be more overt or active.

Based on this understanding, overt methods are more applicable when the need to detect or evade a potential surveillance effort overrides any considerations regarding the need to remain discreet. However, unless the target has reason to suspect that there is a surveillance effort present with immediate hostile intent, the more sophisticated approach to surveillance countermeasures in most cases is to execute them in a manner that does not disclose that the target is surveillance-conscious. As we will see in the next section, the target has many more options and can exploit many more vulnerabilities against a surveillance effort that does not suspect that the target is surveillance-conscious and is practicing surveillance countermeasures.

Given this perspective, if a surveillance countermeasures technique is intended to be effective while not being detected as such, there is a lower *threshold* for how

active it can be before it fails to achieve the desired effect. Alternatively, if the need to detect or evade a potential surveillance effort overrides any considerations regarding the need to remain discreet, then there is no threshold for how active or overt the surveillance countermeasures technique can be. The threshold that applies to a given target is dependent on the overall objectives of the surveillance countermeasures effort.

One key component of the surveillance countermeasures objective that should never be ambiguous to the target is whether he wants to ensure that countermeasures employed are not detected by a surveillance effort as such, or if he is not concerned that the countermeasures will be identified as such. There is no gray area between these considerations, because the implications and consequences on any future intrigue between the target and the surveillance effort are so diametric.

Therefore, based on varying objectives, the covert-overt spectrum is relative to the desired results. With few exceptions, it will be in the target's best interests, at least initially, that the surveillance effort not suspect that the target is surveillance-conscious or practicing surveillance countermeasures. However, there are circumstances when the need to determine for certain whether surveillance is present overrides these considerations. For example, protective services personnel providing security for a high-risk target may be extremely overt in attempting to detect or evade surveillance.

In the end, it is difficult to gauge how active a given surveillance countermeasure can be before it causes an unintended effect or is altogether counterproductive. Variables such as the size and sophistication of the surveillance effort will also impact where this threshold resides. Regardless, the threshold for where the most active measure the target is willing to risk in order to ensure that the surveillance countermeasure is not detected probably runs from the middle to the low end of the covert-overt spectrum. Since the generally more sophisticated, security-savvy target is more limited in his active surveillance countermeasures options than the unconstrained target, he must employ a more sophisticated process to achieve the desired results, rather than rely on the execution of individual overt techniques.

A final consideration in where along the covert-overt spectrum a surveillance countermeasure should be employed involves the classic fight-or-flight response. As with many factors surrounding the surveillance and countermeasures battle, there are a number of psychological factors that apply just as they do in the most savage expanses of the wild. The fight-or-flight response (also called the "acute stress response") simply means that an animal has two options when faced with danger: it can either face the threat (fight) or it can avoid the threat (flight).

Generally, a surveillance effort will place a higher priority on security than it will on maintaining contact with the target, and will therefore choose flight over fight. However, it is important to understand that in some cases—depending largely on the ultimate intent of the surveillance effort—an overt surveillance countermeasure that is identified as such may force the surveillance effort into the fight mode. Any surveillance effort that continues coverage despite knowing that it has been compromised represents an immediate threat to the target, warranting extreme antisurveillance, antipursuit, and protective measures. The most extreme consequence involves an effort that perceives that it has been compromised and is compelled to react in a high-risk or violent manner, rather than run the risk of not having another opportunity with the target. For example, a surveillance effort that is following a VIP

in order to determine where the target would be most susceptible to attack and kidnapping may react by moving directly into the attack phase of the operation if it observes actions by the target that may indicate that he is attempting to detect or elude surveillance

SURVEILLANCE COUNTERMEASURES PRINCIPLE:

SURVEILLANCE DETECTION ENABLES ANTISURVEILLANCE

Active surveillance detection techniques can be effective antisurveillance techniques

This principle is based on the valid premise that most surveillance efforts will want to remain discreet and will therefore terminate contact rather than mirror the target's surveillance detection maneuvers in a readily detectable manner. Therefore, overt surveillance detection methods are also effective antisurveillance methods against a security-conscious surveillance effort. Generally, the more *active* (overt or aggressive) the surveillance detection technique employed, the more likely it will be detectable as such by the surveillance effort, and will force it to either terminate the surveillance or pursue the target despite knowing it is compromised.

Whenever a surveillance detection technique is addressed this concept should be considered as well in order to determine the antisurveillance implications. Most surveillance efforts make operational security their highest priority, because if the target becomes aware of coverage, the surveillance effort is severely hindered or rendered completely ineffective. Any surveillance effort that places a higher priority on maintaining security than it does maintaining contact with the target will normally terminate the surveillance after observing the target execute a surveillance detection maneuver, rather than risk further compromise. Even the most subtle active surveillance detection maneuvers can "spook" a particularly sensitive surveillance effort. For example, with a highly security-conscious surveillance effort, restrictive terrain may serve as an antisurveillance deterrent in and of itself, by forcing the effort to terminate contact rather than commit assets into a potentially compromising situation.

Consistent with the discussion of the previous principle, the degree to which overt techniques are employed must be tempered by the fact that a point is reached at which the technique is counterproductive from the surveillance detection standpoint because it will only serve to force the surveillance effort to terminate contact. If the overall objective is to detect surveillance without the surveillance effort knowing that it has been compromised, then an active surveillance detection maneuver that serves an antisurveillance function is counterproductive. In most cases, it will be in the target's best interest that the surveillance effort not terminate contact prior to being confirmed as such. For this reason, the target must effectively regulate where along the covert-overt spectrum the method will fall in order to achieve the acceptable risk/benefit ratio that best meets the objectives.

By way of summation, active surveillance detection techniques can place the surveillance effort in a position that forces it to either terminate the surveillance or risk compromise, making them effective antisurveillance techniques as well. *However, this demonstrates that the intended technique (surveillance detection) has an*

unintended result (antisurveillance) This also demonstrates that surveillance countermeasures that give the surveillance effort the ultimate choice ("terminate contact or risk exposure") are suboptimal. As will be discussed in the conclusion of the section, what is optimal is the employment of surveillance countermeasures processes that incorporate techniques to *manipulate* and *exploit*, and can be executed in incremental stages that are more effective in achieving the desired results, while not being overtly identifiable as such.

SURVEILLANCE COUNTERMEASURES PRINCIPLE:

ANTISURVEILLANCE ENABLES SURVEILLANCE DETECTION

Antisurveillance techniques can also be very effective in achieving the objectives of surveillance detection.

This principle is based on the fact that a surveillance effort that attempts to maintain contact, despite overt antisurveillance efforts by the target, will readily expose itself to surveillance detection. Generally, antisurveillance techniques are executed in a manner that forces the surveillance effort to terminate contact rather than risk exposure to likely detection. For the most part, antisurveillance techniques gain their effectiveness based on the fact that most surveillance efforts will place a higher priority on maintaining security than they will on maintaining contact with the target. Therefore, overt antisurveillance measures are most effective as long as the surveillance effort is not willing to overtly mirror the target's antisurveillance measures in order to maintain contact.

Antisurveillance is the most difficult surveillance countermeasure to conduct discreetly because the techniques are generally more aggressive and readily identifiable by a surveillance effort. Again, the more overt or active the antisurveillance maneuver, the more effective it will be in eluding or evading surveillance. However, against a determined and capable surveillance effort, only the very most overt techniques will be singularly effective in evasion.

Additionally, these techniques will not meet the overall objective of most targets, as they will be immediately identified as active antisurveillance efforts. For these reasons, antisurveillance techniques employed in isolation, and not as part of a process, are generally ineffective. Unless the immediate need to detect or evade a surveillance presence overrides all other objectives. Again, except under extreme circumstances, an effort to achieve immediate results at the expense of the broader objectives is generally the exception and not the rule.

As with the previous principle, this demonstrates that the intended technique (antisurveillance) can lead to an unintended result (surveillance detection). Although there is an obvious surveillance countermeasures benefit to detecting the surveillance effort, in the event that a surveillance effort attempts to maintain contact after the target executes antisurveillance maneuvers, it should indicate either that the surveillance effort is tactically unsound from the operational security perspective, or that it is determined to maintain contact despite compromise.

The latter is an immediate concern, as any surveillance effort that continues coverage despite knowing that they have been compromised represents an imminent threat to the target, warranting extreme antisurveillance, antipursuit, and protective

measures. Aggressive antisurveillance techniques that do not force the surveillance effort to break contact are the very most effective surveillance detection techniques, but in virtually all cases, the most important factor that they confirm is that the target is in immediate danger.

This possible eventuality certainly demonstrates that surveillance countermeasures that give the surveillance effort the ultimate choice (terminate contact or risk exposure) are suboptimal. In this case, the target has given the surveillance effort the choice (or compelled it) to continue with the surveillance or pursuit rather than avoid compromise and detection. By conducting antisurveillance techniques that give the surveillance effort a choice (fight-or-flight), the target has orchestrated a situation that may lead to the most dangerous of unintended consequences.

THE PROCESS APPROACH TO SURVEILLANCE COUNTERMEASURES

The principles addressed in this section provide an opportunity to substantiate the broader issue of executing procedures incorporating appropriate techniques, as opposed to employing isolated techniques as the means to an end. This underscores the true challenge and art of surveillance countermeasures, as the target can never truly "reduce the hunter to the hunted" unless the tables can be turned without the surveillance effort knowing that this has been achieved. The lone exception to this is when the antisurveillance objective is neutralization, which will be addressed in the final section of this manual.

The fact that active or overt techniques are more effective in achieving immediate results does not necessarily make their utilization the most effective surveillance countermeasures strategy. While overt techniques may be effective in achieving immediate goals, they are normally not in the best interests of meeting the longer-term objectives of most targets. If an overt surveillance detection technique fails to detect surveillance but does force the surveillance effort to terminate coverage, the technique was not effective and was very likely counterproductive to the target's overall objectives. If an overt antisurveillance technique fails to evade a surveillance effort, it was certainly not effective and has likely been counterproductive by either inducing the fight response, or compelling the effort into a pursuit.

Overt surveillance countermeasures that are identified by the surveillance effort as such basically force the surveillance effort to make a choice. Whenever the surveillance effort is provided the opportunity to make a choice, the target has relinquished control of the surveillance countermeasures process to the adversary. Not only has the target shown his hand by demonstrating surveillance consciousness, but he has also given the surveillance effort the choice regarding how the next stage of the confrontation will proceed.

Recalling the chess analogy from the Introduction, this is the classic situation wherein the target may doom himself to eventual "checkmate" by seizing the opportunity for an immediate tactical gain. Whether the intended result of a given surveillance countermeasures technique is surveillance detection or antisurveillance, by allowing the surveillance effort the option, the target will very likely not achieve the intended result.

As a final note, the discussion in this section should not be taken to imply that the execution of active surveillance techniques is not appropriate, because they are essential to the execution of effective surveillance countermeasures processes. The main point is that active surveillance countermeasures techniques should not be employed in isolation as an expedient, except when circumstances dictate that aggressive measures be employed based on immediate security concerns. Rather, active surveillance countermeasures techniques should be employed at the time and place of the target's choosing, and as a component of an integrated process.

Surveillance Countermeasures Concepts

INTRODUCTION

As stated in the introduction to this manual, the methodologies, techniques, and procedures presented herein represent concise applications of the very most effective surveillance countermeasures based on a comprehensive analysis of hostile surveillance threats. To this point, the theory and practice of surveillance operations and surveillance countermeasures have been detailed in order to provide a basis for the guiding concepts of surveillance countermeasures.

Based on the analysis of the art and science of surveillance countermeasures principles within the context of the standard surveillance operations methods, key guiding concepts have been derived that scope the development of the primary and most effective surveillance countermeasures techniques and procedures. This section introduces two key concepts that represent the basic components to this methodical approach to surveillance countermeasures. These concepts establish the cornerstone for virtually all surveillance detection and antisurveillance tactics and techniques, and are summarized as follows:

1 Surveillance Countermeasures Concept: Be Inconspicuous

In most cases, and at least initially, it is to the target's advantage that the surveillance effort not suspect that the target is surveillance-conscious or practicing surveillance countermeasures.

2 Surveillance Countermeasures Concept: Target Pattern Analysis

A surveillance effort conducts target pattern analysis to maximize the efficiency and security of the surveillance operation.

A thorough appreciation of these fundamental concepts is essential to the basic understanding of surveillance countermeasures techniques and procedures, and will be referred to throughout this manual, particularly as they apply to the next level of surveillance countermeasures, which are the more specific surveillance detection and antisurveillance procedures.

Concept Summary

The concepts of *be inconspicuous* and *target pattern analysis* are interrelated as they apply to establishing the conditions for effective surveillance countermeasures. Even if surveillance is suspected, whenever feasible it is best initially to maintain a normal pattern of activities without demonstrating any indication of surveillance consciousness or raising suspicions. In this way, the surveillance effort, if present, is allowed to develop a sense of confidence and security regarding its strategy for

surveillance coverage of the target based on target pattern analysis. This also enables the target to assess his own patterns of activities to understand how any surveillance effort would develop and implement a surveillance strategy.

If indications of surveillance are identified through passive surveillance detection, or otherwise, the target can begin to develop a surveillance countermeasures strategy based on the situation. An appreciation of the surveillance threat's target pattern analysis process will enable the target to determine when and where the most effective surveillance countermeasures can be employed.

SURVEILLANCE COUNTERMEASURES CONCEPT: BE INCONSPICUOUS

In most cases, and at least initially, it is to the target's advantage that the surveillance effort not suspect that the target is surveillance conscious or practicing surveillance detection.

Generally, a surveillance effort will adjust its coverage based on how surveillance-conscious the target is observed or perceived to be. If the surveillance effort assumes that the target is not surveillance-conscious, it will likely be less security-conscious in the employment of tactics and the exposure of assets. This should provide better opportunities for the target to detect surveillance. Conversely, if the surveillance effort suspects that the target may be surveillance-conscious, it will exercise greater operational security and will provide the target fewer opportunities for passive observation.

In most cases, a recognizable effort at surveillance detection or antisurveillance will cause the surveillance effort to adjust its tactics or terminate the surveillance altogether. In either case, the result may be counterproductive in the sense that, even if the surveillance effort is not terminated, it may become more sophisticated and much more difficult to detect. Since a primary objective of surveillance detection is to isolate surveillance assets for observation, retention, and subsequent recognition, the termination or enhancement of surveillance coverage could negate opportunities to confirm surveillance by observing surveillance assets at subsequent times and locations.

A final reason for remaining inconspicuous is that it sends a message to a surveillance effort, if present. Any experienced surveillance effort will be very cognizant of surveillance consciousness on the part of the target, unless surveillance countermeasures are executed in a very subtle and effective manner. Generally, surveillance is conducted against a target in order to develop some type of information. A display of surveillance consciousness on the part of the target will be perceived as an indication that he has something to hide.

A surveillance effort will likely intensify its coverage—and perhaps increase the number of assets—if it perceives that the target does have something to hide, and will generally assume a more secure and cautious posture if it suspects that the target is surveillance-conscious. For this reason, any premature activity by the target that heightens the surveillance effort's sensitivities will be counterproductive, as it will place the effort on alert and make it less susceptible and vulnerable to unexpected surveillance countermeasures techniques and procedures.

Although the target may not have the luxury of "waiting out" a surveillance effort, in many cases the best defense against a surveillance effort is to make it unprofitable.

Regardless of the surveillance effort's motivation and capabilities, it will not indefinitely sustain coverage of a target that does not demonstrate activity of operational interest in support of the objectives of the surveillance operation

SURVEILLANCE COUNTERMEASURES CONCEPT: TARGET PATTERN ANALYSIS

A surveillance effort conducts target pattern analysis to maximize the efficiency and security of the surveillance.

In an earlier section we addressed *target pattern analysis* as an element of an effective surveillance operation. This factor becomes a key concept that can be exploited for surveillance countermeasures purposes. Based on target pattern analysis, the surveillance effort will tend to develop a sense of security by relying on established patterns to dictate its coverage strategy. Over time, a surveillance effort may be drawn into a sense of complacency that can be readily exploited at the time and place of the target's choosing. When this sense of security is suddenly disrupted by an unanticipated maneuver on the part of the target, the surveillance effort may be forced to react in a manner that leaves it vulnerable to detection.

The effective application of surveillance countermeasures exploits the surveillance concept of target pattern analysis to develop specific strategies to detect or evade a surveillance effort based on the target's self-examination of established patterns of activity. This process enables the target to determine when and where during his routine travel patterns the surveillance effort may be vulnerable to a surveillance countermeasures maneuver, or series of maneuvers.

Surveillance countermeasures maneuvers that are significantly inconsistent with the established patterns will be readily apparent as such to a surveillance effort. For this reason, the target's appreciation of his own target pattern analysis profile is necessary for the development of surveillance countermeasures procedures that would appear more plausible to the surveillance effort, if present.

The Chaos Theory of Surveillance

INTRODUCTION

A key factor in the effectiveness of surveillance countermeasures is the degree to which the surveillance effort is caught surprised, off-balance, or in a compromising position. Although there are a number of situations that can cause such effects for instructional purposes, ACM IV Security Services captures many of the intangibles of a surveillance operation and refers to this dynamic as The Chaos Theory of Surveillance. This application epitomizes the concept of manipulation and is among the most effective means of reducing the hunter to the hunted.

In mathematics and physics, Chaos Theory addresses the phenomena of how isolated events can destabilize systems. This theory is commonly referred to as the “ripple effect,” and is probably most popularly associated with the “butterfly effect,” which suggests that the flapping of a butterfly’s wings might cause tiny changes in the atmosphere that ultimately cause a tornado to appear.

A surveillance effort employs a systematic approach that involves common tactics, techniques, and procedures. Whether the surveillance effort is a single person or multiple operators, there is basically a set system of methods that the effort will apply in reaction to the target’s movements. With multiple operators, this systematic approach becomes even more important, because each individual operator needs a good understanding of how all the operators can be expected to react to a given situation. This ability to understand how each operator can be expected to react is what makes surveillance a system. The Chaos Theory of Surveillance and its destabilizing effects, are as applicable to a surveillance effort as the Chaos Theory of physics is to any other systematic approach.

The psychological and physiological factors of confusion, anxiety, friction, inertia, and momentum apply to any surveillance operation. Ironically, even the majority of individuals categorized as “professional surveillance operators” are actually unaware of the advanced concepts that impact most surveillance operations. Such “professionals” understand that these dynamics occur, but have never conducted a critical analysis of the problem to identify the root causes and corrections. These factors that impact a surveillance operation based on confusion, inaction, or overreaction are addressed as they apply to The Chaos Theory of Surveillance, which, if effectively exploited, is the ultimate manipulation of a surveillance effort for isolation, detection, or evasion purposes.

CHAOS THEORY DISCUSSION

Within the surveillance professionals’ community, surveillance operations are affectionately characterized as *hours of boredom periodically interrupted by moments of chaos*.

This tongue-in-cheek characterization implies that even an unwitting target can cause a noteworthy degree of chaos for a surveillance effort. The hallmark of a professional surveillance effort is its ability to react to and manage chaos. However,

chaos that is deliberately created by a manipulative target can be virtually impossible for even the most capable surveillance efforts to manage. Consistent with the above characterization of a surveillance operation, the target can orchestrate moments of chaos to isolate, manipulate, and exploit surveillance assets—hence the term *The Chaos Theory of Surveillance*.

The course of a standard surveillance operation generally involves the surveillance effort monitoring and recording the target's mundane day-to-day activities. Particularly in the case of a target that does not demonstrate surveillance awareness or consciousness, the surveillance effort will observe the target's routine activities that will likely remain consistent over the course of days and even weeks. This is where target pattern analysis, whether conducted as a formal process or developed repetitively over a period of time, tends to settle the surveillance effort into a sense of security and in some cases overconfidence. Over time, a surveillance effort may be drawn into a sense of complacency that can be readily exploited at the time and place of the target's choosing. When this sense of security is suddenly disrupted by an unanticipated maneuver on the part of the target, surveillance assets may become isolated and even forced to react in a manner that leaves them vulnerable to detection.

When the target conducts an unanticipated activity that is not consistent with target pattern analysis, the surveillance effort will likely assume that the unusual activity is potentially of very high operational interest, since it deviates from established norm. This professional instinct to ensure that contact is maintained while at the same time reacting to an unanticipated event, if effectively exploited, renders the surveillance effort vulnerable to isolation and detection. As a synergistic effect, the laws of psychology and physics can be exploited to cause a situation that is chaotic for the surveillance effort, yet controlled by the target.

Any number of intangible factors build up over the course of a surveillance operation, but two general categories of factors that develop and can lead to poor execution in the face of uncertainty are referred to as *inertia* and *friction*. These elements, in conjunction with the generation of "momentum," are factors of vulnerability that the target can manipulate against the surveillance effort.

The inertia of a situation is accentuated by destabilizing factors such as the adrenaline of the moment, fear of losing the target, and a drive to accomplish the objectives. In this context, inertia is action based on a general sense on the part of surveillance assets that there is a need to move and react, but an uncertainty regarding exactly what needs to be done. This movement amid confusion and without sound direction is readily exploitable for surveillance detection and antisurveillance.

There are also factors—such as an anxiety about avoiding compromise and even sleep deprivation—that can tend to generate a destabilizing friction. As a potentially debilitating counterbalance to inertia, friction is inaction or hesitation. This is a tendency of some surveillance assets to err on the side of being overcautious under uncertain circumstances. An interesting point is that, in a given situation, surveillance assets may react differently. This can result in a combination of inertia and friction that causes variations in momentum and negative momentum that can very readily desynchronize and compromise a surveillance effort.

APPLICATIONS OF THE CHAOS THEORY OF SURVEILLANCE

The number of exploitable applications of this theory is infinite, and they will differ based on whether the objective is surveillance detection or antisurveillance. Given this understanding, a basic example provided for illustration purposes involves the target traveling to his workplace. Assuming a surveillance presence, the surveillance effort will have likely performed some target pattern analysis and will be aware of the target's standard route to work. As such, as the target progresses along the route to work, the surveillance effort will assume that it is a routine phase of the surveillance, with the target conforming to his established pattern.

As the target is in the final approach to his work location, he can initiate the Chaos Theory by continuing past the work location (or by deviating just prior to reaching it) when the surveillance effort is relaxed and fully anticipating the conclusion to another standard phase of the operation. This will immediately launch the surveillance effort into a reactive mode when it is probably poorly positioned based on the final preparation for the stop and the fact that it is now faced with uncertainty based on this new and irregular activity. At this point, any number of maneuver options are applicable to further exploit the inertia, friction, and general chaos that such a basic action can cause if properly executed.

As with the number of specific surveillance countermeasures, the possible applications of the Chaos Theory are unlimited. In fact, if not for the serious nature of a potentially hostile surveillance effort, the target could "toy with" a surveillance effort using various chaos-inducing methods. Transition points such as temporary stops, transitions from vehicular to foot surveillance, and transitions from foot to vehicular surveillance also provide abundant opportunities to orchestrate chaos scenarios.

The combination of Chaos Theory dynamics with concepts and techniques to be addressed in subsequent sections, such as the "temporary break in contact," "avoid lost contact, and "lost contact reaction" are indicative of a security professional operating at the "master's" level of the trade.

There is no professional surveillance operator with street-level experience who would dispute that such a Chaos Theory exists. Virtually no "professionals," however, have ever examined the phenomenon in detail to understand the alpha and omega of this dynamic, though all have experienced it. This stands as another example of the higher level of understanding needed to master the art and science of surveillance countermeasures. Once again, tactical applications are standard fare, but an understanding of advanced concepts such as The Chaos Theory of Surveillance enables the target to enter, manipulate, and disrupt the hostile surveillance threat's decision cycle and operational process.

Surveillance

Countermeasures

Applications:
Manipulation

Isolation Overview

INTRODUCTION

Isolation is an incremental process that is best characterized as a methodical effort to distinguish potential surveillance assets from the surrounding environs for observation and subsequent *exploitation* as appropriate. The importance of isolating surveillance assets can not be overstated: it is the critical path to effective surveillance countermeasures. The term “isolation” has connotations that could imply a method of “entrapment,” but this is actually the most extreme case. Despite this caveat, the methods of isolation do in a sense transition the target’s role from the “hunted” to the “hunter.”

With very few exceptions, isolation is a prerequisite for effective surveillance countermeasures. Isolation is first and foremost a method of manipulation in support of surveillance countermeasures. The most effective surveillance countermeasures procedures consist of a manipulation stage and an exploitation stage. The manipulation stage is an incremental process of isolation techniques. The isolation process ranges from the initial isolation efforts to identify specific indications of a surveillance presence to the more focused techniques intended to isolate specific surveillance assets in preparation for exploitation. The closing isolation techniques for the most effective surveillance countermeasures procedures generally consist of the target inducing the surveillance asset into a situation or position making it vulnerable to a directed exploitation measure.

The techniques employed to isolate surveillance assets are similar for surveillance detection and antisurveillance, but the combination of techniques employed in a given procedure may vary. Although surveillance countermeasures procedures can be executed in a deliberate manner over hours, the execution of most procedures can be measured in minutes, and in many cases, seconds. This demonstrates that a well-developed and well-executed surveillance countermeasures procedure will efficiently employ a succession of isolation techniques leading to the decisive isolation technique that establishes the conditions for a definitive exploitation effort.

Once potential surveillance assets have been isolated, and depending on the surveillance countermeasures objective, the target can then execute a specific isolation technique as part of a surveillance detection procedure to enable the definitive confirmation of surveillance, or as the basis for manipulation in the initial stage of an antisurveillance procedure. Coincidentally, as we will see in Part V, the most effective manipulation techniques in support of both procedures are the same.

Isolation is a means to achieving detection, but it is not synonymous with detection. Surveillance detection is achieved either by multiple sightings of surveillance assets or by observing for conspicuous actions or reactions that indicate or confirm a surveillance presence. In either case, this requires that potential surveillance assets be isolated for scrutiny and testing. Recall that for any surveillance detection maneuver to be effective, the target must be able to observe the reaction to the maneuver. By first isolating the potential assets, the target can then focus his observation to ensure the detection of surveillance.

The initial isolation technique is invariably based on the surveillance imperative of *maintaining contact*. The incremental process then progresses from the general to the more specific through a succession of mutually built-upon techniques. For example, if the target is traveling down a multilane road, he can essentially isolate potential surveillance assets by observing the general grouping of following vehicles in the positions that a surveillance asset might occupy if present. The general isolation of a grouping of potential surveillance assets would be the initial isolation technique to focus follow-on isolation techniques.

Although in many cases isolation and detection is a progression toward antisurveillance, there are circumstances in which isolation can be much less precise and complete for antisurveillance than is necessary for surveillance detection. Although the degree of isolation depicted in the previous example is certainly not rigid enough for definitive surveillance detection, just the appreciation of where the potential following surveillance assets might be is a sufficient degree of isolation if antisurveillance is employed as a standard security practice, even with no specific indications of a surveillance presence. Granted, most sophisticated antisurveillance efforts would require a greater degree of isolation as a precondition, but this is not always the case.

Isolation Methods

Isolation is a primary component of the manipulation stages of the most effective surveillance countermeasures procedures. Isolation techniques are initially executed to identify potential surveillance assets, and then as the final form of manipulation in order to exploit for definitive surveillance detection and antisurveillance purposes. As they apply to surveillance countermeasures, isolation techniques have three distinct isolation purposes:

- 1 Isolation techniques to identify potential surveillance assets
- 2 Isolation techniques employed as an element of a surveillance detection procedure to detect or confirm a surveillance presence.
- 3 Isolation techniques employed as an element of an antisurveillance procedure to evade or elude a surveillance presence

The *isolation purpose* to identify potential surveillance assets (1) is the precursor and the basis for follow-on isolation techniques in support of the most effective surveillance detection (2) and antisurveillance (3) procedures. As it applies to isolation purpose objective (3) above, a section of Part V (“The Break and Disappear Antisurveillance Procedure”) will pull it all together into the definitive antisurveillance procedure.

As they apply to surveillance detection, once potential surveillance assets are isolated, the most effective procedures to exploit the potential assets involve using one or a combination of the following *exploitation methods*:

- 1 Observe for retention and later comparison, or to compare with previously identified suspected assets.
- 2 Elicit a compromising response
- 3 Execute a surveillance detection maneuver, or series of maneuvers, to elicit a compromising response

Exploitation method (1) above (observe for retention and later comparison, or to compare with previously identified suspected assets) is a standard surveillance awareness practice and can stand as a key component of a surveillance detection procedure that will be discussed further in Part V (“The Temporary Break in Contact Surveillance Detection Procedure”).

Exploitation methods (2) and (3) apply to isolation purpose (2) above. The amalgam of these aspects form the manipulate-to-exploit transition in the definitive surveillance detection procedure, which will be detailed in Part V (“The Temporary Break in Contact Surveillance Detection Procedure”).

ISOLATION TECHNIQUES INTRODUCTION

This section addresses the techniques that are employed to isolate potential surveillance assets and is a logical continuation of the isolation methodology

addressed in the previous section. Effective surveillance detection requires that potential surveillance assets be isolated for detection. There are three primary categories of techniques through which surveillance assets are isolated:

1. The detection of indications of mirroring. Techniques designed for this purpose are based on the fact that in order to be effective, a surveillance effort must employ the two basic imperatives of maintaining contact and mirroring.
2. The exploitation of restrictive terrain based on an understanding of how restrictive terrain impacts freedom of movement and how a surveillance effort will react to compensate. Techniques designed for this purpose are based on the fact that the exploitation of restrictive terrain is an effective means of isolating a surveillance effort for surveillance countermeasures purposes.
3. The exploitation of transition stages based on an understanding of how a surveillance effort operates in reaction to these stages and the inherent vulnerabilities to isolation. Techniques designed for this purpose are based on the fact that the transition stages of a surveillance operation present observable and exploitable profiles that can result in unique vulnerabilities to surveillance countermeasures.

While the concepts behind these three techniques will be discussed in detail, recall that Part II addressed the imperatives of contact and mirroring, transition stages, and restrictive terrain with applications to surveillance countermeasures. To avoid repetition, readers should refer to Part II as necessary to augment the information provided as it applies specifically to isolation.

ISOLATION TECHNIQUES CONCEPT OVERVIEW

The imperatives of maintaining contact and mirroring are key guiding concepts for surveillance countermeasures. The irony is that these are such simple concepts, but they are the ones on which the advantage turns to either the “hunter” or the “hunted.” The reality is that the imperatives of maintaining contact and mirroring are significant constraints under which the surveillance effort must operate in order to succeed. In fact, the only way that a surveillance effort can succeed under these conditions is if the target is unaware and its efforts go undetected. With a surveillance-conscious target, the constraints imposed by these two imperatives will guarantee that the operation ends in either early termination or compromise.

Due to the nature and vulnerabilities of a surveillance operation, mirroring is the most readily identifiable aspect for surveillance detection. At the passive surveillance detection level, transition stages can force a surveillance effort into detectable mirroring actions or other conspicuous actions to maintain contact, and restrictive terrain can assist in facilitating the isolation and detection of mirroring assets as well. To put it in terms of a mathematical formula, the first category of isolation techniques (detection of mirroring) is the constant, and the other two categories (restrictive terrain and transition stages) are variables that can be employed to exploit the imperatives of contact and mirroring.

At the more active level, the target may maneuver in a manner that makes mirroring actions by surveillance assets, if present, more pronounced and readily detectable. The occurrence of transition stages in the target's travels will have a plausible purpose, but will actually be planned and orchestrated to support either surveillance detection or antisurveillance. The target will also plan the use of restrictive terrain in a manner that enables him to exploit it against the surveillance effort in order to enhance surveillance detection, or support a break in contact with the surveillance effort for surveillance detection or antisurveillance purposes.

Isolation Techniques Concept: Contact and Mirroring

In order to be effective, a surveillance effort must employ the two basic imperatives of maintaining contact and mirroring.

This concept applies to the employment of surveillance countermeasures techniques ranging from the most basic to the most sophisticated. Again, if not for this simple concept, it would not be necessary for a surveillance effort to become vulnerable to isolation or detection in the first place. The concept of mirroring employed in conjunction with the requirement to maintain contact accounts for the large majority of the more effective surveillance detection techniques. The understanding and application of this concept applies to establishing the preconditions for antisurveillance as well.

In the most basic sense, a surveillance effort exposes itself to the possibility of detection only in order to maintain contact with the target. In fact, it is those efforts to maintain contact with the target—even when the surrounding terrain and environment do not facilitate cover and concealment—that render a surveillance effort most vulnerable to surveillance detection. It is also the surveillance effort's attempts to anticipate the target's actions in the form of mirroring that may leave it vulnerable to surveillance detection.

Although the detection of mirroring by a surveillance-conscious target can be effective in isolating possible surveillance assets, it will normally not be until the target executes an active surveillance detection measure that the target will be able to confirm surveillance. In many cases, this active measure will be a maneuver to induce an asset into mirroring in a conspicuous manner that confirms surveillance.

In Part II, "Surveillance Operations Overview," we addressed mirroring as it applies to the mobile surveillance follow. In basic terms, mirroring implies that a surveillance effort will travel along the same basic route as the target and at the same basic rate of speed, or pace. In addition to the fact that mirroring presents a detectable profile, it also generally implies that a surveillance asset must maintain a steady pace with the target to maintain a comfortable and secure following distance. This pace obviously impacts the pace of any other surveillance assets involved in the follow.

This dynamic, referred to as pacing, is among the most exploitable from a surveillance countermeasures perspective. By gradually fluctuating the travel pattern by pace and positioning, the target can observe for vehicles or pedestrians that mirror the same pattern. When maneuvering aggressively through traffic, the target can observe for vehicles that are also traveling behind in an aggressive manner. Conversely, by traveling in a slow and conservative manner, the target can observe for vehicles that conform to this pattern as well.

One final aspect of mirroring as it applies to isolating potential surveillance assets is the exploitation of traffic patterns and traffic flow. In many locations, the majority of the traffic tends to flow in one primary direction based on time of day or other circumstances. Vehicular and foot city commuter traffic is the most common example, but there are many other circumstances that would dictate traffic flow, such as special events and many forms of restrictive terrain. In the appropriate locations, surveillance assets that continue to mirror the target's movements when traveling against the natural flow of traffic are readily isolated from the surrounding traffic for surveillance detection purposes. Traveling against the natural flow of traffic can also present a traffic obstacle that can be exploited for antisurveillance purposes.

Isolation Methods Concept: Transition Stages

The transition stages of a surveillance operation present observable and exploitable profiles that can result in unique vulnerabilities to surveillance countermeasures.

As addressed in Part II, transition stages (or transition points) provide unique opportunities for surveillance detection. Whether it be the transition among the box and follow stages of a surveillance operation, or between vehicular and foot surveillance, the transition points are junctures in the operation that render surveillance assets vulnerable to isolation due to the actions necessary to maintain contact while in transition. At the most basic level, transition points can render a surveillance effort vulnerable to isolation based on the transitions from a static to mobile or a mobile to static posture. At the more advanced level of understanding, transition stages can be employed as decisive points to implement Chaos Theory measures for both surveillance detection and antisurveillance.

The mere understanding of how a surveillance effort establishes a hasty box during temporary stops is a vital perspective. Recall that there is a *window of vulnerability* for the surveillance effort while it maneuvers to establish a hasty box when the target stops.

This also represents a surveillance countermeasures *window of opportunity* for the target. In keeping with a sound understanding of The Chaos Theory of Surveillance, the target can immediately assume the offensive by stopping and then reinitiating movement before a surveillance effort would have had the opportunity to establish secure box positions. From the surveillance detection perspective, the target can then direct efforts to isolate potential surveillance assets based on an understanding of the logical box positions that surveillance assets would be expected to assume.

In particular, the transition from vehicular to foot surveillance enables the isolation of potential assets and provides a number of possible surveillance detection options as discussed in Part II ("Transition Stages—Vehicle to Foot" and "Open Terrain"). Again, the risk to surveillance detection by foot is a general lack of protection and a limited ability to rapidly evade (accelerate away from) danger. While not always applicable to high risk threats, the transitions among vehicular and foot surveillance present a number of challenges for a surveillance effort, primarily involving vulnerabilities to isolation and "lost contact." The vulnerabilities of detection that are inherent to the Box as previously addressed are accentuated when this is coupled with the difficulties involved in the transition from a foot to a vehicular surveillance.

Isolation Methods Concept: Restrictive Terrain

The exploitation of restrictive terrain is an effective means of isolating a surveillance effort for surveillance countermeasures purposes.

Again, restrictive terrain serves primarily to isolate the surveillance effort by forcing assets into areas that restrict freedom of movement or negate cover and concealment. Methods that lead surveillance assets into restrictive terrain are common methods of isolation. Some specific applications of restrictive terrain were discussed in detail in Part II.

Given the requirement to maintain contact with the target, restrictive terrain will usually force the surveillance effort to assume additional risk of detection in order to ensure that observation of the target is maintained. Surveillance vehicles may tend to close their following distance when approaching traffic hazards or obstacles such as highway interchanges or busy intersections in order to maintain observation through the obstacle. After passing the hazard, surveillance assets will tend to return to a more discreet following distance. This tendency to push in, coupled with mirroring, serves to isolate possible surveillance assets.

Open terrain is exploited to negate cover and concealment, which in turn negates freedom of movement and serves to isolate surveillance assets for detection. Open terrain forces a surveillance effort to make a trade-off between line-of-sight observation and how closely it chooses to maintain contact with the target. When the surveillance effort chooses close contact over distance, it makes itself immediately vulnerable to detection. The term "open terrain" as it applies to foot surveillance can also include areas that negate cover, not necessarily by forcing operators into the open, but by forcing them into areas where they are denied a plausible "cover for action" and therefore stand out.

Any terrain or obstacle that serves to canalize, condense, or otherwise restrict a surveillance effort can be effective in isolating assets. The most basic and common tactical employment is the "logical 180-degree turn." This tactic is most effectively employed for surveillance detection purposes when the target has isolated potential surveillance assets in terrain that restricts their options to react in a natural and plausible manner when the maneuver is executed.

Having been isolated with limited options to react, surveillance assets will be forced to pass by the target head-on or better yet from the surveillance detection perspective—be compelled to make a hasty and conspicuous effort to *avoid* a head-on confrontation, which serves to virtually confirm surveillance.

As a caution, although *traffic obstacles* can support surveillance detection and antisurveillance, there are risks involved that must be considered. The use of traffic obstacles such as dense city traffic or other congested areas such as road construction sites, exploit the fact that a following surveillance effort will be hindered in its movement by the obstacles.

The same constraints or restrictions that apply to the surveillance effort, however, will also apply to the target when traveling through the obstacles. For this reason, it is important to ensure that by using these techniques, the target is not traveling into a situation that could restrict his escape options and make him more vulnerable to attack. The employment of intrusion points to draw potential surveillance assets into close proximity with the target for isolation and exploitation purposes presents

the greatest risks in this regard. These are particularly important considerations if the surveillance countermeasures employed may force the surveillance effort into a “fight-or-flight response” situation.

The Break in Contact

The break in contact is a key enabling element for both surveillance detection and antisurveillance procedures. Since it does involve the execution of multiple techniques, it is a procedure in and of itself, but as we will see in Part V, it is best employed as a key stage in the most comprehensive and effective surveillance countermeasures procedures.

As will be addressed in Part V ("The Temporary Break in Contact Surveillance Detection Procedure"), the purpose of effecting a break in contact for surveillance detection is to consciously allow surveillance assets, if present, to reestablish contact in a manner that isolates them for detection. Also in Part V ("The Break and Disappear Antisurveillance Procedure"), we will see that the primary purpose of effecting a break in contact for antisurveillance is to facilitate the subsequent execution of maneuvers to confound a potential surveillance effort's attempts to reestablish contact. In either case, the break in contact is executed in order to manipulate the surveillance effort based on an understanding of how it thinks and reacts.

Just as the term "break in contact" implies a loss of observation by the surveillance effort, it must be executed in a manner and location that enables the target to execute follow-on maneuvers that the surveillance effort cannot observe. The employment of a "blind spot" is most germane to this concept and will be addressed in Part V ("The Temporary Break in Contact Surveillance Detection Procedure"). For antisurveillance purposes, an immediate period of "lost contact" is necessary to conduct follow-on maneuvers to confound attempts by the surveillance effort to regain contact.

Whether the objective is surveillance detection or antisurveillance, the methods employed to effect a break in contact are basically the same. The primary difference between the two is the location and circumstances under which the break in contact will be executed. The options for overt maneuvers to break contact are plentiful, but as previously discussed, these can be counterproductive if the surveillance effort perceives the activity as blatant surveillance countermeasures. If executed properly, a break in contact establishes the preconditions for effective surveillance countermeasures, based on the objectives.

The key point to understand is that the break in contact is most effectively employed as an integral stage of either a surveillance detection or antisurveillance procedure. Therefore, since it is a stage in a process, and not a means to an end in and of itself, it can be employed in a more subtle and inconspicuous manner if properly executed. The key components that facilitate effective break-in-contact efforts are pacing, acceleration, transition stages, and restrictive terrain.

Pacing

An advanced understanding and application of pacing applies to its use as a method of manipulation to generate momentum on the part of surveillance assets that can be exploited against them. A large part of a break in contact can be summarized succinctly as *using the surveillance effort's momentum against it*. Since the surveillance effort, or individual assets thereof, will accelerate and decelerate at a pace

that is generally consistent with that of the target, the target is in essence dictating the pace of the surveillance effort. Although this concept may seem obvious, the effect is that this enables the target to control the tempo of the surveillance effort and, when appropriate, exploit the tempo against it.

In other words, the target can induce surveillance assets to either accelerate or decelerate, and then use that momentum against them for surveillance countermeasures purposes. By manipulating or controlling the pace or tempo of the surveillance effort, the target can slow the pace to generate "negative momentum" to establish the preconditions for a break in contact. The application of pacing coupled with open terrain can establish among the most suitable conditions to effect a break in contact.

Acceleration

In many cases, acceleration is a key component of any procedure involving a break in contact. In fact, many basic efforts to break contact with a surveillance effort can be categorized as "accelerate and escape." This is another excellent example of how techniques used in isolation—rather than as part of a process—are less effective and in some cases counterproductive, depending on the surveillance countermeasures objectives. Employing a strategy of acceleration alone as a means to escape or break contact will likely be perceived as a surveillance countermeasure and will therefore be less effective than measures combining multiple aspects. By combining actions that might be characterized as "accelerate and escape" with other enabling measures, the end result is a more effective and discreet surveillance countermeasures effort.

The pacing discussion above reflects how acceleration employed as a component of a process is more effective. By inducing (manipulating) surveillance assets into "negative momentum" and then using acceleration (ideally in conjunction with other components), the target can break contact while also convincing the surveillance effort that the reason for the lost contact was its own overcautiousness or poor tactical judgment. When acceleration is incorporated in a process approach, the surveillance effort will be more inclined to perceive the reason for a break in contact as a result of its own judgment regarding how to conduct the follow, and less likely to perceive it as an active surveillance countermeasures effort.

Transition Stages

Transition stages (points) provide a multitude of opportunities to break contact with the surveillance effort. A surveillance effort will rely on target pattern analysis or other methods in an effort to predict the target's most likely or logical actions during the preparation for or reaction to transitions stages. For this reason, transition stages provide many of the best opportunities to apply The Chaos Theory of Surveillance by performing an unanticipated action in conjunction with a transition stage.

Recall that there is a *window of vulnerability* for the surveillance effort while it maneuvers to establish a hasty box when the target stops. This also represents a surveillance countermeasures *window of opportunity* for the target. This window of opportunity enables the target to go on the offensive by stopping and then reinitiating movement before a surveillance effort would have had the opportunity to establish

secure box positions. This dynamic facilitates a break in contact with a desynchronized surveillance effort.

Even a well-established box presents vulnerabilities to the surveillance effort when the target begins to transition from a static to a mobile status. When the target departs the box, surveillance assets must pull out into traffic to establish the follow. Obviously, the faster the target is moving, the more difficult it will be to establish positive contact in the follow in a timely manner. This method can be readily employed to force a break in contact in support of surveillance detection or antisurveillance. Although this method does largely employ the element of acceleration, the fact that it is coupled with a transition stage makes it more discreet and effective.

Also recall that in establishing a box, coverage of the potential routes of travel will be prioritized based on the target's most likely utilization. When the number of possible routes exceeds the number of available surveillance assets, this prioritization drives which routes will be covered by assets and which routes will not be covered.

This prioritization may be based on target pattern analysis, but will more likely be based purely on a situational assessment of the target's most logical routes of travel. Given this understanding, the target can use reverse logic to confound the surveillance effort by traveling from the box location along a route that would likely have been given a low priority for coverage.

The transition from vehicle to foot surveillance is one of the most effective situations for effecting a break in contact. In fact, the options available by foot, particularly in crowded public locations, provide many opportunities to elude a surveillance effort. The transition from foot to vehicular surveillance involves the vulnerabilities addressed as they apply to the transition from a vehicular box to a follow, coupled with the difficulties involved with this transition. An effective chaos-inducing method is for the target to execute a stop that would require the surveillance effort to transition from a vehicular to a foot status, and then force a transition back to vehicular surveillance while the surveillance effort is still in the process of executing the initial transition.

Restrictive Terrain

Although restrictive terrain is primarily exploited in support of surveillance detection as an *isolation* method in and of itself, the obstacles characterized by many types of restrictive terrain can also be exploited to effect a break in contact that will in turn support other active surveillance detection or antisurveillance measures. In fact, with a determined and aggressive surveillance effort, obstacles that physically impede movement may be the only means to facilitate evasion.

In many cases, the use of restrictive terrain to affect a break in contact is most effective when combined with the component of acceleration. The target should accelerate prior to entering restrictive terrain or traffic obstacles to increase distance from the surveillance effort, and accelerate out of the traffic obstacle when complete to further increase separation while the surveillance effort is still obstructed by the obstacle. Open terrain can also be exploited to force the surveillance effort to increase its following distance (reverse momentum), which can in turn be exploited by acceleration and evasion to achieve a break in contact. The exploitation of traffic flow

as a traffic obstacle, by traveling against the natural flow of traffic, can also facilitate “break in contact” efforts

Surveillance

Countermeasures

Applications:
Exploitation

Introduction to Surveillance Countermeasures Procedures

The final part of this manual consists of two surveillance detection procedures and two antisurveillance procedures. It is important to note that of the procedures detailed, the surveillance detection procedure ("The Temporary Break in Contact Surveillance Detection Procedure") and the antisurveillance procedure ("The Break and Disappear Antisurveillance Procedure") are endorsed as the most effective surveillance countermeasures procedures available. The other surveillance detection procedure ("The Multiple Sightings Surveillance Detection Procedure") is a common one but it also serves as a good contrast with the more progressive and effective procedures.

Two procedures can be viewed as ingenious in their simplicity, but are frequently endorsed as the most effective available. One may question why all the technical theories, principles, concepts, and techniques that have been presented in this manual lead to only one definitive procedure for surveillance detection and one definitive procedure for antisurveillance. At the most general level, the information detailed in this manual is important for any security professional or individual with surveillance countermeasures concerns.

More specifically, a procedure is a sequence of techniques executed within a process to achieve a singular objective. As such, the procedures are broad in application and can be executed employing the range of available isolation and exploitation techniques. In fact, variations of these very procedures could be executed repeatedly against the same surveillance effort, and if orchestrated properly, would repeatedly provide plausible reasons for each episode. Once again, by playing on the individual or collective psyche, and given a logically plausible explanation, a surveillance effort will tend to rationalize and perceive these episodes as unanticipated anomalies rather than surveillance countermeasures.

As a final note of introduction to Part V, the second antisurveillance procedure ("The Temporary Break in Contact Antisurveillance Procedure") is one that most targets will choose not to employ, but it is a fitting conclusion as it truly epitomizes the edict of "reducing the hunter to the hunted." While this section does have great instructional and anecdotal value, it is a radical departure from the rest of this manual. In light of this, it is important to note that while this manual concludes with this section, the primary emphasis of this manual is to demonstrate how the hostile surveillance can be defeated with procedures that manipulate and exploit through techniques driven by discretion, ingenuity, and sophistication, and not through procedures employing overt actions and engagement.

The Multiple Sightings Surveillance Detection Procedure

INTRODUCTION

Tactical applications for surveillance detection techniques are well documented, but there is little in the way of documenting methodical surveillance detection procedures. However, one procedure that is well understood and widely employed among security professionals is the multiple sightings surveillance detection procedure. While this procedure involves a much more sophisticated methodology than the simple execution of individual techniques in isolation, it is still a very basic process that will not satisfy the overall surveillance countermeasures objectives of most targets. The fact that this procedure is the one that is most commonly addressed demonstrates a general lack of perspective regarding the concepts addressed in this manual and their application to the comprehensive surveillance countermeasures procedures that will be addressed in the following two chapters.

Perhaps the most deliberate and time-consuming form of isolation is observing for indications of the same surveillance assets in multiple locations. The multiple sightings surveillance detection procedure involves efforts to isolate surveillance assets for observation, retention, and subsequent recognition. As such, the objective is for the target to essentially isolate the surveillance effort over time for exploitation through observation. This procedure for isolation and detection is feasible only when the need to confirm surveillance is not immediate and the risk of hostile action is assessed as low, and is the procedure of choice only when that target has the latitude to conduct surveillance countermeasures activities in a more passive manner over time.

Although a very common surveillance detection procedure, the multiple sightings surveillance detection procedure is very basic in application and assumes that the target will be given multiple opportunities to observe for potential surveillance assets.

In many cases, however, the target will not have the time or want to accept the risk of a deliberate and perhaps lengthy process of detecting surveillance through multiple sightings. In fact, the most progressive surveillance detection measures are those that enable the target to cut straight to the determination of whether or not a surveillance effort exists.

This procedure is introduced as the opening of the Exploitation section of this manual despite the fact that it is not proactive enough to meet the requirements of most targets. Although there is some instructional value, the more interesting purpose that this discussion serves is to demonstrate a significant contrast between this most common procedure and the more proactive, decisive, and definitive surveillance detection and antisurveillance processes in the following chapters. As such, these more comprehensive procedures will underscore just how basic and conservative this widely employed procedure actually is.

THE MULTIPLE SIGHTINGS SURVEILLANCE

DETECTION PROCEDURE

In the context of *exploit* and *manipulate*, this procedure involves the repetitive execution of two basic steps

- 1 Isolate (manipulate)
- 2 Observe (exploit)

This procedure relies heavily on the proper execution of isolation techniques, because effective isolation is necessary to facilitate the primary means of exploitation which is observation. In many cases, this form of isolation not only focuses on potential surveillance assets, but also involves a process of elimination to reduce the number of suspected assets to be isolated. To this end, isolation surveillance detection techniques as previously addressed are employed to observe and identify the same surveillance assets (individual or vehicle) at multiple locations. Of course, the more illogical it is that the same potential asset would be observed in the vicinity of the target at two or more locations, the higher the likelihood of surveillance.

Isolation through multiple sightings may be sufficient to confirm surveillance, or the target may choose to direct an active surveillance detection maneuver at a given suspected asset to ensure that the suspicions are not a mistake or mere coincidence. In this sense, this procedure can serve as a more deliberate isolation process in support of the more decisive surveillance countermeasures procedures detailed later in this chapter.

Although this is generally considered a more time-consuming and deliberate procedure, there are applications that enable a more progressive approach. The employment of a surveillance detection route (SDR) with preplanned surveillance detection points (SDP) is the most condensed and focused application of the procedure.

SURVEILLANCE DETECTION ROUTE

A surveillance detection route (SDR) is an advanced method of surveillance detection that is performed to induce a surveillance effort into mirroring the target's broad movements in a manner that facilitates the isolation and multiple sightings of surveillance assets. Whether developed graphically on a map or mentally, the SDR applies the understanding of surveillance detection concepts and principles to specifically planned maneuvers along a given route.

In most cases, an SDR will incorporate active surveillance detection maneuvers throughout that are executed in locations that maximize the observation of surrounding traffic at their points of execution. The ultimate objective of an SDR is to execute sequential detection maneuvers that will initially identify potential surveillance assets and subsequently isolate those assets to confirm a surveillance presence.

The most effective yet complex form of SDR is one that incorporates a theme to make an otherwise illogical route of travel appear logical. Common themes involve traveling to numerous stores as though pricing a particular item. Another effective theme is to plan an SDR around properties listed in the paper and use the guise of property hunting as a logical reason for an otherwise illogical route of travel. The

theme stop locations represent the surveillance detection points (SDPs) where the target will observe (exploit) for potential surveillance assets. Additionally, restrictive terrain and transition points along the SDR can serve as SDPs.

One of the more basic SDR applications is the “three sides of a box” technique. This concept is applicable in many situations, and does not need to be executed in a linear fashion as the name implies. The concept behind this technique is that the target will travel from one point to another by *not* taking the most direct and logical route. A very basic “three sides of a box” technique, such as employing it in a street block, is as much a mirroring detection technique as it is for multiple sightings, but a more elaborate “three sides of a box” technique over a larger area would be executed to facilitate multiple sightings.

Figure 1 is a very simple example of this concept using a box that can portray a city block or other potential SDR area.

For illustration purposes, assume that the target, suspecting surveillance, is approaching point A from the bottom of the box. If point D is the target’s intended destination, he would turn right at point A and travel directly to point D. However, as a form of surveillance detection, the target will take an illogical route along the “three sides of the box” from point A through points B and C to reach point D. Any vehicle that is observed following the target through this indirect and illogical route is immediately identified as a possible surveillance asset.

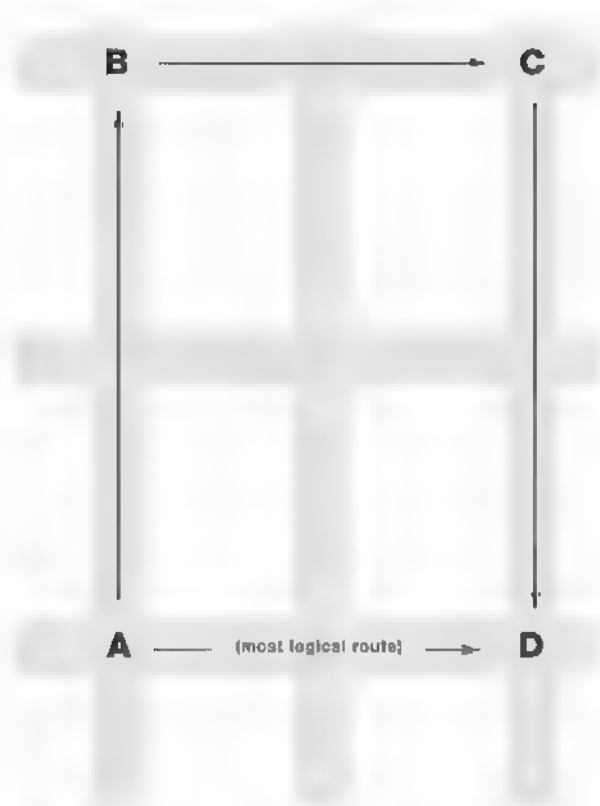


Figure 1

Although the example in Figure 1 is the simplest possible application and may even be perceived by a surveillance effort as an overt detection maneuver, the concept is applicable in a number of variations whether the target is traveling by foot or vehicle. As such, the easier the surveillance effort is able to detect that the target is employing the method, the more likely it will be to break off prior to compromising itself. Therefore, the better planned and less discernible the technique, the more likely it will be to succeed and the less likely that it will be perceived as a detection maneuver.

In most cases, countersurveillance support (third-person surveillance detection support) will be planned and executed around an SDR with SDPs.

The Temporary Break in Contact Surveillance Detection Procedure

INTRODUCTION

Isolation can be a means to an end, but more likely will be the precursor to the execution of situation-dependent surveillance detection maneuvers. The most proactive and effective technique to facilitate isolation is the “temporary break in contact.” For surveillance detection purposes, the most effective application of the temporary break in contact is as an element of “the temporary break in contact surveillance detection procedure.” To varying degrees, all the concepts addressed to this point can be employed at some level to enable the execution of this procedure, which is invariably the most important surveillance detection weapon in the arsenal.

It is important to note that while the concepts of “contact and mirroring,” “transition stages,” and “restrictive terrain” apply directly to the isolation of potential surveillance assets, they can also be employed to enable a temporary break in contact. Even an understanding of target pattern analysis can be applied to determining when and where a surveillance effort may be most vulnerable to efforts to “break contact.”

Of particular note, the relationship between The Chaos Theory of Surveillance and the temporary break in contact surveillance detection procedure is tantamount to applying theory to practice. Recall that if not for the serious nature of a potentially hostile surveillance effort, the target could exercise elements of the Chaos Theory to “toy with” (manipulate) a surveillance effort. There is no other application that better reflects the characterization of “toy with” than the temporary break in contact surveillance detection procedure, as it can truly make the target a “master of puppets” in regard to potential surveillance assets. Like no other surveillance detection procedure, this one *manipulates* the surveillance effort in a manner that transforms it from the hunter to the hunted.

The most effective application of the temporary break in contact surveillance detection procedure consists of the target, through his actions, creating a situation in which the surveillance effort fears that it may not be able to observe the target as he passes through a traffic option. The desired response that this should elicit is that the surveillance effort reacts in an aggressive manner to avoid a “lost contact drill” situation. It is this reaction to regain contact prior to the option, in an effort to avoid a lost contact drill situation, that isolates the surveillance assets and sets the stage for this most effective application of surveillance detection.

Recall from our “Isolation Overview” discussion in Part IV that the most effective procedures to exploit the potential assets for surveillance detection purposes will employ isolation techniques to either “elicit a compromising response” or “execute a surveillance detection maneuver (or series of maneuvers) to elicit a compromising response.” In the context of *manipulate* and *exploit*, the temporary break in contact surveillance detection procedure can be summarized as follows:

1. Isolate (manipulate)

- 2 Break in contact (manipulate)
- 3 Isolate (manipulate)
- 4 Observe (exploit)
- 5 Directed action (exploit) as necessary
- 6 Observe (exploit) if directed action is employed

THE AVOID LOST CONTACT CONCEPT

The temporary break in contact surveillance detection procedure finds its effectiveness based on the "avoid lost contact concept." This is yet another classic example of how the seemingly complex disciplines of surveillance detection and antisurveillance can be broken down into such simple components. Just as the imperatives of contact and mirroring are extremely simple once examined, this basic cause-and-effect method of isolation for surveillance detection purposes is ingenious in its simplicity as well.

Unlike the isolation technique categories previously discussed, the avoid lost contact concept does not directly isolate surveillance assets, but it does facilitate isolation. The strength of this concept is the fact that it is based on an understanding of how a surveillance effort thinks and reacts, making it among the most effective from the surveillance detection standpoint. The concept is as follows:

When placed in a situation that risks losing contact with the target, a surveillance effort will take aggressive, and sometimes extreme measures to regain contact with the target.

The avoid lost contact concept makes the temporary break in contact surveillance detection procedure effective. Like no other concept, this is the one that truly plays on the "psyche" of a surveillance effort. Understanding that surveillance assets will react in an aggressive and potentially compromising manner to avoid a "lost contact" situation is a priceless perspective as it applies to surveillance detection.

This concept most regularly applies to the risk of losing contact with the target when approaching a traffic option. The sense of urgency that immediately besets a surveillance effort when it loses contact with the target is among the most exploitable for surveillance countermeasures purposes. Recall that a surveillance effort will execute a lost contact drill if the target is not observed as he reaches a traffic option or other location at which he could have taken any number of possible directions of travel. Regardless of the number of assets for any surveillance effort, the lost contact drill is a circumstance to be avoided if at all possible, because the consequences of losing contact with the target are significant. For instance, even if contact is regained during the course of the lost contact drill, a surveillance effort with multiple assets will become dispersed and will be at a disadvantage until it is able to reconsolidate the effort.

The concept of "avoid lost contact" is a significant element of the mastery of surveillance detection tradecraft. This level of insight enables the target to essentially assume control of a situation by simply exploiting the psychological impact that individual instances of lost contact have on a surveillance effort. From the team (peer) perspective, an individual surveillance operator who is responsible for allowing a lost contact situation that results in a lost contact drill has essentially failed himself and his team. The psychological motivation to avoid this fate alone generates the "inertia" and "momentum" that drive surveillance assets into positions of isolation within the

target's range of observation. Even a surveillance effort involving only one operator shares this psychological impact of the desire to avoid failure.

Regardless of the size of the surveillance effort, the motivation not to lose contact with the target is most directly related to overall mission objectives and the need to maintain contact versus the other considerations, such as vulnerability to compromise. In other words, if a surveillance effort is involved in a more deliberate and long-term mission, it will be less inclined to overreact to a potential lost contact situation, while an effort with a more immediate short-term objective will be more aggressive in ensuring that contact is maintained. Of course, while the latter is more susceptible to manipulation and isolation, it is likely a greater immediate threat to the target as well.

TEMPORARY BREAK IN CONTACT SURVEILLANCE DETECTION PROCEDURE

The "temporary break in contact" is perhaps the most effective means of isolating surveillance assets, and in many cases, is a means to the end of confirming a surveillance presence. It is important to understand that this measure does not directly involve a surveillance effort's execution of a lost contact drill. Rather, it exploits a surveillance effort's professional instincts, which are to *avoid* a lost contact situation whenever possible. In fact, it is the surveillance effort's reaction to the possibility of losing contact with the target that renders it most vulnerable to active surveillance detection. As previously noted, anytime there is a break in contact (observation) with the target, there is a sense of urgency to regain contact in a timely manner and prior to reaching a traffic option. Immediately upon a break in contact, the surveillance effort will tend to accelerate in an effort to regain contact. This tendency essentially generates a degree of "momentum" among surveillance assets that is employed against them.

The age-old tactic of turning a "blind corner" and then waiting for the surprised surveillance asset to find himself face to face with the target is a classic example of a temporary break in contact that is as ageless as intrigue and espionage. Although it can be perceived as an overt surveillance countermeasures method if not properly executed, this basic tactical application is among the very most effective surveillance detection methods, and also serves as a good example of the elements of a temporary break in contact surveillance detection procedure. These elements are:

1. Isolate in preparation for a break in contact (manipulate)
2. Effect a break in contact (manipulate)
3. Find a "blind spot" and isolate the surveillance assets when they appear and regain contact (manipulate)
4. Observe for compromising actions (exploit)
5. Execute a surveillance detection maneuver (or series of maneuvers) to elicit a compromising response (exploit as necessary)
6. Observe for compromising actions (exploit) if surveillance detection maneuvers executed

Given an understanding of the dynamics of surveillance involved, the temporary break in contact surveillance detection procedure is simple. The target will break

contact in order to orchestrate a lost contact situation that induces surveillance assets to react by accelerating to regain contact. While out of sight ("blind spot") of the potential surveillance assets, the target will then establish, or reestablish, a rate of travel (or stop altogether) that will enable the surveillance assets to regain contact, but in a manner that enables the target to isolate the surveillance assets based on the fact that they bear down on him in an unnatural manner. In such a circumstance, surveillance assets may further isolate themselves for detection by visibly decreasing speed once they have regained contact. In fact, the best planned temporary break in contact maneuvers will be executed in a manner in which the target finds a blind spot that does not allow following surveillance assets observation of the target until they are virtually on top of him. The desired effect is that when the surveillance asset does catch up to the target, its momentum either forces it to pass by the target in a more natural manner or to decelerate in a conspicuous and detectable manner. When placed in a situation in which an immediate decision is required, many surveillance assets will "freeze" and act conspicuously (the "friction" factor). Ideally, given the appropriate restrictive terrain, the surveillance assets' freedom of movement can be limited in a manner that gives them no option but to bear down on the target and decelerate in a conspicuous manner.

THE "BLIND SPOT"

For perspective, the time elapsed between the break in contact and the isolation of potential surveillance assets in the temporary break in contact surveillance detection procedure is generally measured in seconds. By vehicle, the execution of this technique may be a matter of less than 10 seconds from initiation to isolation and detection. Obviously, the time involved will depend on the terrain and rate of speed, but this perspective is important to the understanding that the blind spot is more of an expedient than an elaborate set of circumstances. In fact, once the target enters the blind spot, it will induce an immediate reaction from surveillance assets if the procedure is properly executed. For this reason, the blind spot can be characterized as any location or situation that causes a short-term loss in contact (observation) that requires movement or action by surveillance assets in order to reestablish contact.

The "blind corner" is a good example for illustration purposes, but tactics and applications based on the same concepts are more accurately referred to as methods that use a blind spot. This distinction is necessary, because there are many locations other than a simple corner with physical structures preventing line of sight that are suitable to create a blind spot that facilitates a temporary break in contact. Perhaps the most common example that also has "detection" applications is that of the policeman nested away with a radar gun in a blind spot where the speeders cannot see him until they are already in range with their speeds recorded.

Recall that surveillance assets will conduct hand-offs to avoid mirroring and to minimize exposure to the target. In fact, this is a standard tactic that is executed for security when the target makes a turn. In virtually all cases, however, there is a varying amount of time—normally seconds—in which no asset will have contact (observation) with the target as the hand-off is executed. This simple factor alone can facilitate any number of variations of the blind spot ("blind corner") method.

The concept of pacing and the target's manipulation of a surveillance effort's tempo in conjunction with the blind spot is the most effective means of isolation in

support of this procedure. While corners may be the most common options to create a temporary break in contact and blind spot situation, there are many other options that can be exploited with equal effect, and in many cases more discreetly. In fact, suitable terrain that facilitates speed variations to manipulate and exploit the tempo or momentum of surveillance assets enables some of the most effective applications of the temporary break in contact surveillance detection procedure.

In areas where there are bends in the road that would force a following surveillance asset to lose sight of the target temporarily (a blind spot), the target can travel at a faster speed going into the blind bend, and then decrease speed when completing it. If successful, this will result in the surveillance assets pursuing quickly around the bend and then bearing down on the target as it completes the bend. This will force the surveillance asset to either decrease its speed in an unnatural manner or pass the target. A poorly disciplined surveillance asset may even decrease its speed to reestablish a secure following distance, which will be highly indicative of surveillance.

This tactic can be used with the same effect when the target travels over the crest of a hill that would temporarily blind following surveillance assets from observing the target's activities after cresting the hill. *Although the blind bend "blind spot" technique may seem intuitively simplistic, with very few exceptions, this technique (or variations thereof) is the single most effective means of surveillance detection ingenious in its simplicity.*

Although some of the best blind spot options have been cited as examples, the possibilities are unlimited. However, for any temporary break in contact exploiting a blind spot to be effective, there must be some type of traffic option at some point within or after the blind spot that would compel following surveillance assets to accelerate in an effort to regain contact. Among the more obvious reasons, a surveillance effort uses maps to look ahead and anticipate hazards. If there is a traffic option ahead of the target, the surveillance effort will be aware of this and react accordingly in the case of a potential lost contact situation.

By foot, the blind spot options are generally more abundant than by vehicle due to less restrictive movement options, but the temporary break in contact isolation technique applications will normally take more time to orchestrate due to the slower rate of speed.

EXPLOIT

The final stage (or stages) of the temporary break in contact surveillance detection procedure is the actual surveillance detection technique that is employed against the potential surveillance effort. Recall again that the purpose of isolating surveillance assets through the temporary break in contact is to either elicit a compromising response or execute a surveillance detection maneuver (or series of maneuvers) to elicit a compromising response.

In many cases, the fact that the surveillance asset suddenly finds itself in a vulnerable position is enough to elicit a compromising reaction. This can be accomplished by simply isolating a surveillance asset in a situation where it feels compelled to react hastily to avoid detection. If isolation alone does not sufficiently compromise the potential asset, it still serves to isolate the asset in order to focus the more active, overt, or aggressive detection measures. Once surveillance assets are isolated, an immediate surveillance detection maneuver will be directed against the

suspected surveillance asset to elicit a compromising reaction and confirm it as such. This constitutes the one-two punch that will normally force even the most savvy and composed surveillance professionals to flinch in a detectable manner.

There are a wide range of possible surveillance detection maneuvers (tactics) available, and the particular maneuver employed will be selected based on the specific situation. The options for possible surveillance detection tactics are virtually infinite, with the most common being well documented in references that deal with this less sophisticated aspect of surveillance detection.

The most aggressive directed surveillance detection techniques are those that essentially force surveillance assets into a conspicuous and detectable reaction. When the target is under the protection of a security detail and this procedure is executed using more aggressive directed techniques, it may be orchestrated in a manner that gives any potential surveillance effort the impression that the target (the detail's principal) is with the detail, when in fact he is not. The fight or flight response has been addressed in detail. The vast majority of surveillance efforts are intended to function as covert and discreet efforts that remain undetected throughout the entire course of a given surveillance operation.

Given this, the effectiveness of the temporary break in contact surveillance detection procedure is based on the fact that the initial and natural reaction for the vast majority of surveillance assets will be to choose "flight" without any consideration given to a "fight" response. In fact, when faced with the prospect of close contact or even a potential confrontation with the target, most surveillance assets will execute "flight," regardless of how conspicuous it may be. In order to avoid such a situation. Although this direct confrontation approach must be tempered with caution, the closer a surveillance asset suddenly finds itself to the target without plausible options for cover, the more likely it becomes that a "flight" response will be forced upon that asset in a manner that will be readily detected by the target.

As it applies to Chaos Theory, the psychological aspects of fear will very often override any consideration regarding being compromised as a surveillance asset. Such aspects range from the fear of detention to the fear of physical harm. While such directed surveillance detection methods are relatively overt and aggressive, they can still be executed in a plausible manner if incorporated with some type of logical follow-through. For example, the target can act in a manner that indicates that he is moving toward a confrontation with a potential surveillance asset, but then continue the feign to a logical conclusion that falls short of, or bypasses, the surveillance asset. From the surveillance detection perspective, this approach is the one that best characterizes the concept of reducing the hunter to the hunted, but the antisurveillance procedure detailed later ("The Break and Disappear Antisurveillance Procedure") takes this concept to its extreme manifestation.

The Break and Disappear Antisurveillance Procedure

INTRODUCTION

This chapter presents a conceptbased antisurveillance methodology that is ingenious in its simplicity. Taken at face value based on the name, the break and disappear antisurveillance procedure sounds pretty simple and straightforward, but in reality and much like the temporary break in contact surveillance detection procedure, it incorporates mutually supportive concepts and techniques that combine to form a master stroke of surveillance countermeasures.

Although the surveillance detection concepts of mirroring, restrictive terrain, and transition stages were addressed primarily as they apply to isolating surveillance assets, we have previously addressed their utility as it applies to breaking contact with a surveillance effort. There is no need to repeat these methods as they apply to antisurveillance, because the general concept of breaking contact is the same. The primary difference is that, unlike efforts to temporarily break contact for surveillance detection purposes, antisurveillance efforts are intended to be complete and enduring.

Recall that all antisurveillance measures are considered active and are the most difficult to conduct discreetly because they are generally more aggressive and conspicuous. To effect a permanent break in contact based on a single tactical application, the method must be singularly effective, meaning that it would be difficult, if not impossible, to execute without being perceived as an overt antisurveillance effort. Again, the consequences of this perception can range from intensification of future surveillance efforts to the immediate transition from a surveillance effort to an active pursuit. For this reason, any technique that makes the antisurveillance effort less detectable as such is to the target's advantage.

The most effective technique to this end is the break and disappear antisurveillance procedure, which is based on an understanding of how a surveillance effort thinks and reacts. This *procedure* is a much more effective alternative to individual antisurveillance tactics that may be effective in breaking contact but are ineffective in disguising the employment of antisurveillance activities. The break and disappear enables the target to elude and evade a surveillance effort by executing the technique in a more subtle multistage approach, as opposed to a single overt maneuver. This is most effective as it involves orchestrating a plausible break in contact that is then followed by the target inexplicably and simply disappearing.

In the context of *manipulate* and *exploit*, the break and disappear antisurveillance procedure can be summarized as follows:

1. Isolate (manipulate)
2. Break in contact (manipulate)
3. Employ reverse logic (manipulate)
4. Evade (exploit)

5 Disappear (exploit)

BREAK AND DISAPPEAR ANTISURVEILLANCE PROCEDURE

The break and disappear antisurveillance procedure methodology is based largely on the following concept

The most effective antisurveillance techniques involve breaking contact, enabled by measures that restrict the surveillance effort's freedom of movement as appropriate, and then manipulating the understanding of how a surveillance effort will attempt to regain contact after the target is lost

Effective antisurveillance measures are generally conducted in two sequential and complementary phases. Just as the name implies, the two stages of the break and disappear antisurveillance procedure are the "break stage" and the "disappear stage"

THE BREAK STAGE

The first stage involves the maneuver, or series of maneuvers, to break contact with the surveillance effort. This translates to the first part of the methodology, which consists of

... breaking contact, enabled by measures that restrict the surveillance effort's freedom of movement as appropriate ...

Earlier we addressed the break in contact as a key enabling element of antisurveillance. Again, the maneuvers to effect a break in contact can be enabled by the understanding and exploitation of concepts such as mirroring (pacing), transition stages, and restrictive terrain. In addition to the other applicable concepts, an understanding of The Chaos Theory of Surveillance will enable the target to expand the effectiveness of antisurveillance efforts.

THE DISAPPEAR STAGE

The second phase of the antisurveillance effort involves the actions taken to further confound and elude the surveillance effort after initial contact is broken. If the target is able to break contact and remain unobserved until reaching the first traffic option that gives him multiple possible routes of travel, then the target enters the second phase of an effective antisurveillance routine. This phase translates to the second part of the methodology, which consists of

manipulating the understanding of how a surveillance effort will attempt to regain contact after the target is lost

This concept is based on the understanding that a surveillance effort will continue efforts to regain contact with the target after it has been broken. For this reason, it is necessary to follow any successful break in contact with immediate follow-on measures to ensure that even the most relentless surveillance efforts are unable to recover.

Once contact is broken with the surveillance effort (actual or suspected), the true "art" of the game comes into play. Again, this is the process of understanding how a surveillance effort thinks and reacts. The "lost contact reaction" concept is the guiding

factor behind this second and conclusive evasion phase of antisurveillance methodology

The Lost Contact Reaction Concept

Effective antisurveillance measures are based on an understanding of how surveillance will react to lost contact with the target in an attempt to regain contact

Recall that the lost contact drill is a standard surveillance technique that involves the systematic execution of a series of maneuvers to regain observation of the target (See Part II). This basically involves the immediate prioritization of the target's likely routes of travel from the traffic option or other point of lost contact. The key point here is that the surveillance assets will search for the target based on his most likely (or logical) directions of travel. Therefore, *the obvious antisurveillance approach is for the target to travel in the most unlikely (illogical) direction from the traffic option*

Once a break in contact is established, the target will then continue with a sequential series of *illogical* travel patterns to further confound any follow-on (logic based) searches by the surveillance effort. Once the target is confident that surveillance has been lost, he will then rapidly travel away from the area where he broke contact, because the surveillance effort will tend to conduct an intensive search of that general vicinity.

It is important to note that whenever a surveillance effort loses contact with the target, it will rarely stop attempting to regain contact until all options have been exhausted. Even in the situation when a surveillance effort breaks contact for security to avoid being isolated in a compromising situation, it is important to understand that in most cases, contact is only relinquished to avoid a single instance of compromise, but every effort will be made to attempt and regain contact after the potentially compromising situation has subsided. Anytime the target achieves a break in contact for antisurveillance purposes, it must be immediately followed by a series of evasive maneuvers conducted to confound any follow-on efforts to regain contact.

THE BREAK AND DISAPPEAR

ANTISURVEILLANCE PROCEDURE: PRACTICAL APPLICATION

Figure 2 depicts a symmetric overview of city street blocks. The target orchestrates a Break in Contact intended to ensure that he remains unsighted by any potential following surveillance assets as he enters the traffic option at Point A. Assuming that his most logical route of travel would be to continue straight toward Point B and his next most logical option would be to turn right toward Point C, the target will take the least likely and logical route toward Point D. Again, the determination of prioritizing possible options is based on target pattern analysis of the target's most likely route of travel.

For example, if traveling toward Point B is the most logical route to the target's residence and target pattern analysis would indicate that the target was likely en route home when contact was lost, the surveillance effort would conduct its lost contact drill based on this assumption. In this example, Point C would be the direction of the most likely alternative route to the target's residence or may be a direction that target

pattern analysis indicates that the target may travel if he is not going directly home, for instance to stop at a store or to get gas

Even assuming that the surveillance effort has at least three assets to cover the three possible routes of travel, the target should be able to remain unsighted when reaching Point D, because the route he is on was given the lowest priority and was not taken until the third surveillance asset reached Point A. At Point D, the target will again take the least likely and logical route, which in this case is back toward Point E. At Point E, the target should not turn back toward his original route but should continue to take traffic options that are the opposite of the direction in which it is assumed that the surveillance effort would prioritize its search. This would involve a meandering pattern that generally takes the target out of the area of lost contact, traveling in the direction of Point G.

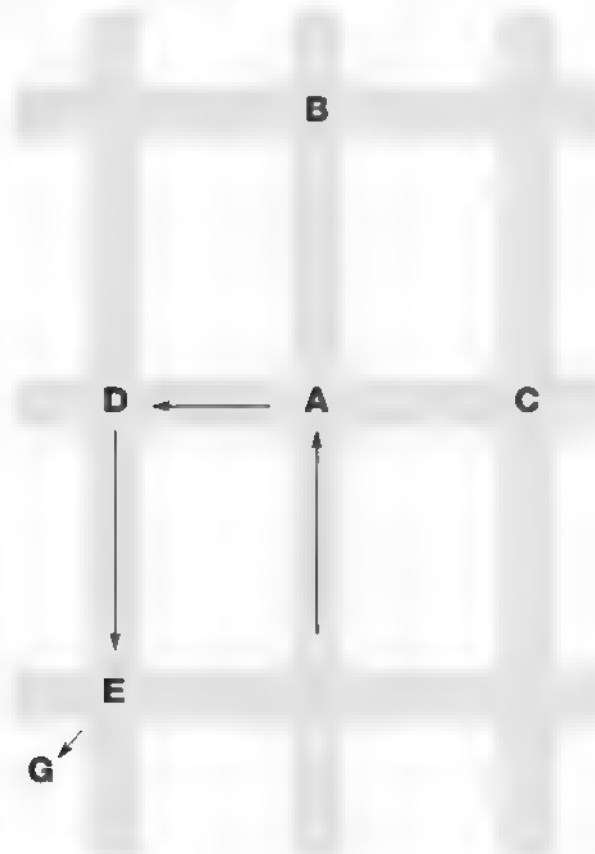


Figure 2

For perspective, it is interesting to understand the metrics of how rapidly the break and disappear antisurveillance procedure degrades a surveillance effort's capability. With this simple example, every option (points in the figure) through which the target

remains unsighted would require multiples of three in available surveillance assets. For instance, to conduct a minimally effective lost contact drill at the first option (Point A) the surveillance effort would require a minimum of three assets. Any fewer than this, and the target will evade surveillance without contest, again assuming that the surveillance effort searches in the target's most likely routes of travel. When the target remains unsighted at the next option, it requires that the surveillance effort have a minimum of nine surveillance assets to conduct a minimally effective lost contact drill at Point D, again assuming that Points B and C were given the priority and have six assets (three at each) dedicated to searching from those two options.

Therefore, by remaining unsighted through Point D, the target will have exhausted the capability of even the most resourceful surveillance efforts. To further make the point, by remaining unsighted through Point E, an effective lost contact drill would require 27 surveillance assets, which exceeds virtually all possible feasibilities. This example demonstrates how the number of required surveillance assets increases by multiples of three at each option—from three to nine to 27.

Although a sophisticated surveillance effort with the resources to conduct a floating box is generally uncommon, the purpose of employing advanced surveillance techniques such as these is to posture for instances of lost contact as detailed in the practical application above. When the target does have reason to believe that the adversarial surveillance effort (suspected or detected) may possess such capabilities, then a variation of the break and disappear antisurveillance procedure will be executed in a location that would restrict the surveillance effort's freedom of movement to employ advanced surveillance techniques.

Accordingly, targets or security details that operate on a "worstcase" basis would plan to execute this procedure in an area with appropriate restrictive terrain as a standard practice. Among the many examples of canalized or other appropriate terrain to restrict such a capability is for the target to travel on a one-way road with the parallel routes being one-way roads in the opposite direction. The employment of this or any number of other such restrictive measures would likely require some variation to the practical application provided above, but this should require only minor adjustments based on the best available alternatives for the application of reverse logic.

The Temporary Break in Contact Antisurveillance Procedure

INTRODUCTION

A general theme throughout this manual has been the employment of intelligence and finesse to defeat a hostile intelligence threat (brains over brawn). Although this procedure employs the aspects of manipulation that make the temporary break in contact surveillance detection procedure the most effective one available, this procedure is a radical departure from the "finesse" that is characteristic of the exploit stages of the other surveillance countermeasure procedures. To this point, antisurveillance has been addressed primarily as a means to elude or evade a hostile surveillance effort. This is in keeping with the requirements and capabilities of most targets. However, there is one other element of antisurveillance that is best generically referred to as "neutralization."

The term "neutralization" has a number of meanings, but as it applies to the temporary break in contact antisurveillance procedure, by neutralizing the surveillance effort the target renders the effort no longer capable of continuing the surveillance. This procedure is designed and intended to force decisive confrontation with the surveillance effort that will terminate the hostile surveillance threat. Potential confrontations may consist of verbal warnings by the target, or the procedure may involve the orchestration of a confrontation with law enforcement elements. Of course, more aggressive confrontations may involve shooting out the tires on surveillance vehicles, sending another type of life-threatening message to surveillance assets such as warning shots, or to the extreme, which is to neutralize the surveillance effort in the most decisive and conclusive manner. Regardless of the method of neutralization employed, this is the surveillance countermeasures procedure that definitively "reduces the hunter to the hunted."

When this procedure is executed by a protective security detail, it will invariably be orchestrated in a manner that gives any potential surveillance effort the impression that the target (the detail's principal) is with the detail, when in fact he is not.

THE TEMPORARY BREAK IN CONTACT

ANTISURVEILLANCE PROCEDURE: MANIPULATE

The manipulation stage of this procedure is identical to the temporary break in contact surveillance detection procedure and consists of the following three elements:

- 1 Isolate in preparation for a break in contact (manipulate)
- 2 Effect a break in contact (manipulate)

3 Find a blind spot and isolate the surveillance assets when they appear and regain contact (manipulate)

The manipulation stage of the temporary break in contact antisurveillance procedure may appear tantamount to drawing the surveillance effort into an ambush of sorts – and this is an accurate account in many ways – but this is also a very simplistic characterization of the process of getting the surveillance effort into the blind spot.

For instance, simply drawing or leading the surveillance effort into areas that restrict options for “flight” and force the “fight” does not take full advantage of the aspects of manipulation that should be available to the target or his security detail. In the context of The Chaos Theory of Surveillance, this does not leverage the aspects of inertia, momentum, friction, and general chaos that are possible.

Just as the aspects of manipulation are employed in the temporary break in contact surveillance detection procedure to achieve a degree of surprise that renders surveillance assets susceptible to detection, the same techniques of isolation and manipulation should be employed with this procedure to ensure that the surveillance effort is as surprised and poorly prepared for the confrontation as possible. Drawing an unsuspecting surveillance effort into an intrusion point is the most extreme measure of manipulation for neutralization purposes.

THE TEMPORARY BREAK IN CONTACT

ANTISURVEILLANCE PROCEDURE: EXPLOIT

This stage consists of one step:

1. Neutralize (exploit)

The target or security detail will only plan to execute a measure of neutralization that he or they are fully prepared for and capable of executing. The techniques executed in the manipulation stage of the procedure will give the target an immediate advantage over the surveillance effort’s assets, but the neutralization technique must be decisive and precise, because this advantage may only be momentary against a capable element that is prepared to rapidly assume the “fight.” As opposed to the other surveillance countermeasures procedures, the range of potential neutralization techniques is more finite, with the final in a succession of escalating options being “extreme prejudice.”

Although such applications are rare and exercised only in the most extreme circumstances, this procedure does epitomize the concept of “reducing the hunter to the hunted.” As a testament to The Chaos Theory of Surveillance, the execution of this procedure with the integration of chaos-inducing techniques is antisurveillance in its purest form, as it immediately, decisively, and without indication terminates the surveillance threat – game over, and they never saw it coming.

Identifying Undercover Activity and Agents

By Timothy W. Tobiason

- 1 Gun Show and General Surveillance Practices
- 2 Personal Experiences with Surveillance
- 3 Differentiating General Public Behavior from HUMINT Collection
- 4 Defense against Surveillance Practices
(Counter Social Engineering)

1. Gun Show and General Surveillance Practices

The United States Government historically has collected enormous volumes of information on its citizens. During the 1960's files were meticulously assembled on political leaders such as Martin L. King, various congressmen, hippies, musicians and the like. Virtually all segments of society were observed, recorded and files on these individuals and groups were assembled and stored. In the event of a major civil uprising, the government had made plans (recently disclosed) to transport "dangerous or subversive" American citizens to internment or concentration camps.

In the aftermath of the Oklahoma City bombing, the US Government increased funding for its law enforcement and intelligence collection agencies and has drastically scaled up its surveillance on its citizens, particularly at gun shows and on citizens who write books they dislike. In light of their intrusive and often illegal activities, I have written and published this book to give ordinary citizens sound information on identifying and countering the "watchers".

The prospect of civil unrest and major civil uprising enhanced by modern science has caused the government to prepare contingency plans for rounding up its citizens and incarcerating them without charges or trial. The reasons for this will be disclosed in this book.

In this chapter we will describe the following –

1. Funding, Scope, and Capabilities of Federal, State and Local agencies
2. Training in conducting Surveillance
3. Deployment for Intelligence Collection
4. Conduct of Undercover Agents

1 Funding, Scope, and Capabilities of Federal, State and Local agencies

Federal agencies that collect and accumulate information on US citizens that may be used for law enforcement and other purposes include the Federal Bureau of Investigation (FBI), Bureau of Alcohol Tobacco and Firearms (BATF), Drug Enforcement Agency (DEA), National Security Agency (NSA), Central Intelligence Agency (CIA), the various armed forces service branches and of course the Internal Revenue Service (IRS)

All these agencies are funded to support staffing of 5,000-15,000 domestic US employees except for the armed forces which can deploy more than one million men and women to needed locations in the US. The staffing numbers are important as you will see shortly. In addition to staffing, travel expenses, firearms, training, supplies and a huge array of surveillance and related equipment are available from a central and regional pools in nearly unlimited quantity for any particular need.

For the purposes of Gun Show surveillance I will use the example of BATF. Although the exact numbers are unknown, I have estimated from congressional reports that all staffing is in excess of 12,000 people. If you divide this figure by an average of 10 gun shows a week this allows for the entire staff to be deployed at a rate of 1,200 per show or roughly broken down into 8 two hour shifts of 150 officers to frequent and monitor the two day weekend shows at any given time.

The cost to the government calculates out as follows -
12,000 employees at \$1,000/wk including travel and expenses
This costs app. \$12 million per week or about \$600 million per year.

The budget allotted for the agencies listed above is actually substantially larger for each one than the \$600 million estimated for BATF here. The additional money goes for high tech equipment, paid informants, training, facilities and so on. During Gun shows I have surmised that an allotment of \$10-20 for cosmetic purposes is allocated to enable agents to blend in by making small purchases thereby mimicking consumer behavior and providing real cover for their intelligence collection activities.

The agents also practice the rewarding of "target" vendors with small purchases when they talk and "open up" to them. This improves their intelligence gathering and effectively conditions the targets to make more money when having a big mouth. Anti government talk is often rewarded since it can be used to inflate the threat and motivate a larger budget from congress.

The other agencies listed each have separate priorities other than Firearms regulation and each assigns agents and supports them in the field according to their prioritized needs. When required, agencies may contribute to a central pool for meeting extra manpower requirements such as the 5,000 table Great Western show in California.

Capabilities of these agents include extensive training and education, decades of experience, and an unlimited electronic potential as the situation demands. This includes all modern forms of bugging, audio, video, infra red and multi spectrum electronics, human informants both paid and voluntary, and use of unwitting 3rd party conscripts. These will be covered in more detail later.

State and local agencies do not have the resources that the federal government has and generally staff at a rate of 250-500 per million population for state highway patrols and about 2-3 per thousand for local populations. County Sheriff staffing varies widely but appears to be 1-2 per thousand population.

2. Training in conducting Surveillance

Surveillance is not conducted at the Federal and professional levels by just going to a target site and wandering around. An overall plan is produced centering around a basic pattern and supported with use of a variety of signals and communications much like a basketball or football team, or a military unit would use.

Individual training includes teaching the following -

- a) Good listening skills Being able to listen to things that you might find offensive, painful, and dangerous without giving away who you are and what you are doing. This can include looking at a book while pretending to read it and being able to listen to the gun transaction taking place four feet away. You learn to examine a gun across the aisle while doing the same thing. The key here is to avoid hint of emotion or heightened interest which might give you away.
- b) Learning deception and lying This means being able to tell people that you are someone you are not. An entire body of science has been developed to teach the body language, vocal skills, temperament and language of how to be convincing when you are actually lying (this author has seen so much of this, that I have concluded that the science of lying is institutionalized within the government to such a degree that it would be nearly impossible for me to sit on a jury and believe anything that a government employee would say against any citizen. That is why we use juries and demand things like evidence rather than just testimony to convict people that the government accuses of crimes.)
- c) Relating and using scripted behavior and conversation. In dealing with professionals, or a suspect with special interests, agents are trained to learn the language and knowledge of the particular interests of the target. They will bring up subjects that are believed to be interesting or of particular momentary interest such as car problems if their vehicle has broken down (especially if the breakdown was deliberate) or a popular television program or movie that the target likes.

- d) Use of body, eye and hand signals This is important when working in groups. At a gun show, if an agent hits a "hot" conversation, they may scratch behind one ear to call for reinforcements in listening to the conversation. This allows the agents to flood a spot and overhear important deals being made or discussed at gun shows. Agents are also trained to move and flow together so that each one picks up part of the conversation and it is pieced together later. This allows for the group to mimic the normal flow of traffic in the show without appearing obvious. Eye signals and hand signals are used to control the flow of traffic by the agents when they are following "bomb book buyers" certain foreigners, and the like. A barely noticeable finger wave may be used to tell one agent to walk around him because he is on a hot target and needs to stay in one spot.

3. Deployment for Intelligence Collection

Just like a football team or military unit lines up in a pattern or formation and then follows a play or plan of action, so do the surveillance experts. At gun shows, the agents are sent in using a staggered approach. Several line up at the door and then move into the isles when the show opens. This first group generally follows a snake like pattern moving very casually through the show since their shifts generally run two hours. By spreading out through each isle they can cover the entire floor averaging one agent per 1-2 tables. The added agents needed to fill out the snake formation are slowly sent in every few minutes to blend in with the crowd. The following agents look to the next person in their line and maintain distance while moving through the show, or close and crowd on "targets" according to predetermined hand and eye signals. "Countercurrent" and other complex patterns are also used to conceal organized movement at gun shows.

A second group of agents also enters the show. These are the floaters who move around in what appears to be a chaotic pattern. They look for the anti-government and radical individuals and begin conducting specific target observation and listening, or may just float as an extra manpower reserve for agents who signal for listening help. The use of pagers with number codes is also used with the vibration of the pager alerting the agents who then look at the numbers which can represent an isle, agents, situations and so on.

A third group is also used at the shows. These are usually paid informants who may only know a single agent but are completely unaware of the presence of the rest of the agents. They usually exhibit unusual and high strung behavior which would seem inconsistent with the ordinary field agents who often are not good actors. Many criminals who have practice at lying and fitting into a particular belief system are often used and deployed in this manner. They are sometimes given a wide berth so

they can operate freely. Sometimes they are worked at close range so it appears to others that they are being watched making their cover appear more genuine.

Supervisors are placed through the show to act as "traffic cops" and electronics are used such as wires on selected agents and informants for "hot" cases, or used directly such as the "pen switch" where a customer asks to use a pen to write a check. They turn their back to the target to write the check while another agent talks to and distracts the target. Then they hand the pen back to the target. It can be a similar pen equipped with a radio transmitter or they might simply unscrew your pen and put a tiny transmitter inside it. [Authors Note: Beware the free pen samples you may repeatedly get in the mail. The ones you can't unscrew need to be broken apart with a hammer to find the tiny bugs.]

These same techniques are used when surveillance is conducted in malls, book stores, restaurants, meetings and so on.

4. Conduct of Undercover Agents

If the government has sent its agents to conduct surveillance on you they are not there for their health (or yours). Uncle Sam has concluded that you are a criminal who needs to be watched and busted.

In cases where anti-government individuals or groups are targeted the government agencies adopt several techniques to deal with, discredit, hound, and frame their targets. The main ones are –

- a) Use of disinformation. This is often used to feed hatred, anger, fear and ultimately to provoke individuals or groups into breaking the law. This serves several purposes. The first is to be able to make a headline making bust, the second is to produce dangerous "wackos" that their agencies need so that more money is extracted from Congress to bust them. (This works quite well actually-You need a big bad enemy to get more funding to fight with. This means pay raises, better electronic toys and fame and fortune when you finally get to arrest them.) The third purpose is to be able to utterly discredit the target by taking them to court later and saying "look at the ridiculous things this person believes-They belong in jail and you the jury should put them there because we the government say so and also because they are stupid."

Some examples of this strategy include

1. Feeding the militias with the belief that China or Russia or the UN has deployed thousands or millions of troops on US soil and that we need action to stop it.
2. Spreading the word that the government and not Tim McVeigh blew up the Federal building in Oklahoma City, therefore we should hate and fight the government.

3. The government has UFO's stashed away and is hiding things from the public. Therefore we should do something now

The common theme here is that we should do something now (translated so we can bust your stupid behind and put you behind bars where we the government think you belong) [All of these have been used on me by the Federal agents at gun shows and most of these attempts are laughable]

A small amount of critical thinking will easily prevent most people from following the undercover line and I will address each of the examples here

1. Your Author had access to volumes of classified information during his tenure in the US Navy (I was the custodian for the STIC Pubs, (Scientific and Technical Intelligence Publications) that the CIA and other agencies provided the Navy to help fight with. The key words here are Science and Intelligence which contrary to popular opinion, the military actually has a little of. I can personally assure you that as of October 1999, no foreign power represents the slightest possible threat of land, sea or air invasion to this nation with the possible exception of a general stream of Latin Americans sneaking across the border looking for jobs and a better life

On critical examination, there are several requirements necessary to support a belief of possible invasion. The first of these is actual evidence in the form of troop movements and supporting logistics. A single division requires the sewage, water, housing, training, vehicles, and related infrastructure equivalent to a city of 15,000 people. This would be impossible to go unnoticed by virtually everyone in the same state. Secondly, a sea or air invasion would require the ability of China or Russia to sea or air lift and support huge numbers of troops against very real US military force. This author doubts that China could successfully invade Taiwan without using nuclear weapons and Russia already showed it could not invade either Afghanistan or Chechnya without defeat.

[Authors Note- The US armed Forces do indeed have capabilities that go well beyond what is publicly known. During my tour in the Navy, we knew without any doubt that we could have swept virtually every ocean on earth clear of all enemy forces in a few days, and we had very real reasons to know that this was true. I can assure anyone reading this that if the kid's gloves come off, what the US military is actually capable of if there are no restricting rules is almost unbelievable, and this does not include nuclear weapons.]

2. The notion that Tim McVeigh was not the bomber of the Federal building in Oklahoma City has been argued on several grounds. The most frequent arguments have been brought up to me by undercover agents whom I recognized and personally knew at gun shows.

The main arguments presented have been 1) that the bomb would not have produced the damage pattern seen, 2) that the cavity left in a portion of the building instead of a perfect semi circle was proof of charges placed inside, 3) there was a second explosion 10 seconds afterwards and 4) Tim McVeigh was framed.

Since I have written and/or published over a dozen books on explosives I can talk with at least a small amount of expertise on this explosion. In the armed forces manuals that I published, there are detailed descriptions of damage patterns to buildings, vehicles, windows and so forth based on the distance from and size of the explosive used. The pattern at Oklahoma City was extremely consistent with the described patterns for a 1-4 ton size explosive placed close to the building. The odd bite taken out of a small part of the building could have been due to a column being the last of four legs supporting some large utility on the roof. When the other three legs collapsed into the rubble, the column could be expected to have been pulled into the collapse as well. A reflected wave or gas line running up the column could have produced the same result just as easily and it is a common occurrence in commercial explosions to have unusual effects like that seen. A quick review of the video of two ton bombs used in the Gulf war also produced similar damage and patterns.

The second explosion often occurs in commercial explosions and is most often due to leaking gas that finally reaches a fuel air mixture that permits combustion and is ignited. I do not say these things because I am a fan of the Government or the FBI. I say them because I believe that the evidence shows them to be true.

The final point concerns Mr. McVeigh. It boils down to this- The entire government case says that he obtained approx. 2 tons of Ammonium Nitrate, added fuel to it to make it into a bomb and then used it to blow up the federal building which incidentally killed and wounded all those in the area. This is the entire case summed up in one sentence.

If I were McVeigh and I did not obtain the 2 tons of ammonium nitrate, I would have taken the stand and told them so and that their records of it were false. If I did not convert it to gas when it was used as a bomb then it would have to have either been used as fertilizer on ground which would have been easy to take the stand and argue. Or if it were still in existence and placed in storage somewhere it would have been easy to say it where it was and the entire case is gone instantly. None of these facts were argued and they were the only ones that

were relevant. The only argument presented was that someone else could have done it.

The entire point of all of this is that it is the federal undercover agents who are the most significant promoters of this type of disinformation.

3. The final bit of misinformation I will address and that I have seen undercover agents spout at gun shows and elsewhere has been related to UFO's. As an amateur scientist I am keenly interested in the possible existence of life elsewhere and of the SETI effort to find evidence of it. I am also reminded of a time in the US Navy when I flew on surveillance planes and had civilians insist to me personally that we were UFOs. Their insistence on their being right about this was equivalent to the level of many of the religious belief systems that members always believe they are right about.

I would like to take the time here to describe some science and its military application and how some people might believe they saw a UFO.

In the 1980's, the government deployed a satellite which used a radar/laser system to very accurately measure the average wave height. Water does not compress like air does so that when the current runs into an underwater mountain, the entire wave front is lifted up according to the height of the mountain and then spreads away. This lift can be measured, recorded and then made into maps of the ocean bottom.

In the mid 1970's the US Navy had an unexpected Soviet submarine threat. We could listen and to and track Soviet submarines all over the world and they knew it. We had great confidence in our ability to find and destroy all their subs in all out war and they also knew this. The Soviets came up with the idea of towing their submarines behind their large grain and cargo vessels without turning the operating equipment on making the subs noiseless. The close proximity to the towing vessel would blend the sonar echoes into a single return. The scientific and technical question at this point for the US Navy and other intelligence services is how would one track a noiseless machine moving underwater in these conditions. The obvious threat was a group of towed and silent submarines being able to launch nuclear missiles and strike targets in 30 seconds as well as laying for all the US ships that would try to immediately leave harbor in the event of war.

The basic science approach to this question becomes obvious. When you watch a sub on the surface you can see the water pushed over its bow and it produces a wake as the water spreads away. As the sub submerges, the wake gets smaller and smaller as it goes deeper until it finally disappears. It does not completely disappear. It can't disappear because a small volume of the water will always push straight up at the circular apex and reach the surface before it spreads. This amount gets smaller as the sub goes deeper but it cannot reach zero because the water does not compress. The wave height gets smaller according to

the inverse of the square of the depth. The next paragraph is the obvious conclusion and conjecture that I can draw based upon knowledge of the basic sciences

Based upon this science it is then possible to build measuring equipment that can be mounted on the underside of an aircraft to accurately measure the average wave height and track any moving bulges on the surface. Such an aircraft may look like an upside down AWAC's when deployed and if they caught a glimpse the LFO people would like to believe they saw something, didn't I know what it was and were sure it came from outer space. This author is quite certain of other sources of origin for many of these incidences

a) Disinformation is widespread and used effectively to some extent by the agents as cover. It makes them appear gullible which I am quite sure they are not but they use this technique to turn stupid and other gullible people into criminals. The real criminals here are the government agents

The final point I need to make here is that the government spends a great deal of time and your tax dollars to alter peoples belief systems for their own purposes which is not a real good use of the public's money or trust

b) Framing. This generally comes in two flavors. The first is where evidence is planted to support a bust. This is usually done by using a third party and is never done consciously with recorded surveillance (because they would catch themselves breaking the law) but has been used effectively to put desired targets behind bars

The second type of framing occurs when undercover operatives can entice, provoke, frighten, intimidate or otherwise motivate targets to break the law so they can make their bust, get medals pinned on their chests, get promotions and pay raises and all the other incentives that go with artificially expanding the easy to bust criminal market

In the next chapter I will cite a number of specific personal experiences in which this has been done to me at gun shows and elsewhere. It became so frequent and annoying that at Kansas City and Oklahoma City gun shows I became exasperated with the agents and told them that "I am perfectly capable of killing people, wiping out cities and committing crimes if I desire to do so without any encouragement or assistance from the government of the United States and its undercover agents, Thank you very much!!!"

*In 1979, This author was arrested for carrying a concealed firearm. Ultimately, the jury found me not guilty but while awaiting trial a deputy sheriff by the name of Bill Frazier told me that a deal had been struck between the judge and the Chief of police to send me to the state pen once I was convicted and that the only chance I had to avoid this was to try to take off and hope they didn't catch me. This is one more example of stupid police trying to make bigger busts

2. Personal Experiences with Surveillance

For many reasons already delineated in my previous books and much too lengthy to repeat here I began to write books in 1996-97 on how citizens could build their own weapons to protect themselves from this government and other eventualities. The series was entitled *The Scientific Principles of Improvised Warfare and Home Defense*. In the spring of 1997 I began to attend gun shows to promote my work and began to run afoul of the US Government surveillance network almost instantly.

In the early days I little realized how extensive and dirty some of the US law enforcement agencies could be in their operations but I would soon find out. What I will describe to you here is a condensed form of only a small fraction of the events to which I have faithfully observed, recorded and interpreted. These will be the main highlights of what for me has become an almost daily lifestyle.

My first gun show as a book dealer took place in Kansas City where I soon began to notice that some of the people who came to look at my books did not seem to fit in with the other attendees. They asked questions of why I wrote the books, what my motives were, and generally conducted "soft" interrogation which made it easy to tell the agents apart. Regular consumers don't much care about motives and personal detail, they just want the book and information for themselves. I could count heads with this behavior and estimated only a few dozen agents per show. This would continue for about three months.

During the next three months I would observe the agents clustering around when someone other than their own agents came to look at and buy the weapons books. They would use hand and eye signals to move people around and would often continue the surveillance past my own tables. I concluded that this was where they accumulated their list of possible suspects when bombings take place. Some were followed out of the building and I even commented once to them that I thought it was a bunch of crap.

At about three months into the shows I went to Blaine, Minn. And on a boring Friday night I began to watch the agents many of whom I now recognized personally move around. I had never been to a show in Minnesota so it was surprising to me that I would personally recognize so many of the attendees. It was also surprising that they many of them moved through the show in formation according to a discernible pattern. Then the whole picture seemed to emerge. It was astonishing at first and I felt like a complete idiot that so much organized and planned activity could be taking place around me without my having the foggiest idea of it at all.

Over time the agents adopted a pattern of dealing with my selling books that they did not like. They would send in people to talk with me and sympathize with my feelings, followed by the oddball belief system agents and informants. Then, usually at the end of the show they would send in someone to pretend to be really offended, angry or hurt by the books. The striking example of this was a US Navy SEAL they sent in to give me a hard time about the cover on my books. They sent him in at the end of the show when I was tired and annoyed. I had put an eagle with a trident on the cover of the book and effectively piggybacked on the Navy SEAL emblem. He would pretend indignation and at the Atlanta show he told me that at least he earned his BUD symbol and appeared to be provoking me to a fight. Here I was, a 40 year old gray haired man who was overweight and with knees that hurt so bad I could scarcely walk by the end of the show being challenged by a magnificently trained and conditioned 20 year old special forces expert. He obviously had earned his BUD and was in great shape and trained to kill which I would never dispute. He had not been trained in what the application of science can do to all that muscle, training and ability.

This provocation angered me along with the overall undercover pattern of harassment so in the fall of that year I began to work on my chemical weapons book. Just prior to my releasing the text material on nerve and mustard agents, I told one of the undercover agents that they did not appreciate the power that this kind of knowledge represented. I recited the story of the SEAL and told him flatly that I could with what I know how to build with my own two hands kill more people than every SEAL on the planet combined and the numbers wouldn't even be close. The agent scoffed at me, told me I was practically crazy and walked off. I then released the chemical weapons text. The SEAL was never sent in again and no one ever made fun of my book cover or my statements again.

What did happen is that the US Senate passed the Feinstein bill criminalizing the sale of dangerous weapons books. At the Cleveland gun show, a copy of the bill was placed in my hands and I was basically told that as soon as Bill Clinton signed the bill I would be arrested. The vote in the Senate for the bill was surprisingly unanimous and I would argue with the agents at the show stating the obvious- what they are going to do, make understanding what words mean against the law. Aside from the first amendment, I and many others do not believe that any government should be allowed to tell its citizens what they are or are not allowed to know.

I ended up going to the federal building in Lincoln, Nebr. to ask Senator Hagel's staff when the bill would be signed so I would know when I would be arrested. As soon as I walked in the door the secretary pressed the emergency security button and in seconds the security people disguised in maintenance uniforms came scrambling in. As soon as they found I wasn't there to blow up the place they left. To make a long story short, the bill was killed by the

combined armed services committee and Mr Hagels office was kind enough to call me and let me know this

Concurrent to these events, several other things were also taking place I began to make counts of agents at the shows which began to be easier to do each time I could go to a show in Texas and count the people I knew in the crowd Since I had never been anywhere close to the Texas shows before it allowed me to get a good head count and make further observations of the surveillance practices under somewhat controlled conditions I estimated from this that average deployment per table runs from 2- 6 agents per two hour shift on average A 1,000 table show would draw 200 to 600 agents per two hour shift to ensure good coverage of all activity I quickly presumed that it would be nearly impossible for anyone to illegally buy a gun or conduct any other criminal activity without the government knowing it in this environment

Given these numbers I roughly estimated that about 10-20% of the crowd in winter shows were federal employees and at times the summer shows ran as heavy as 50-90% Not all of these were federal agents A number were local and state law enforcement that attended the shows and exhibited surveillance and consumer behavior that was often distinct and different from the Feds

During this same time frame I became friends with an undercover agent⁹ in Omaha His approach was so off the wall and his stated belief systems so odd that it was hard to be certain what he was It didn't take long to figure out though Whenever we were in a preset location, he would showboat in a way that someone would if they knew they were on camera His personality changed and he enjoyed crowding the conversation and being its highlight He didn't do this in random meetings or discussions which we had away from prepared situations In setup meetings his conversation was scripted which he tried hard to follow rather than being spontaneous and it was here that he resembled the informant agents at the gun shows The final give away occurred when he planned a meeting with me at a cafe and didn't show up Instead there was a woman at the counter who wore a blue dress and had really nice legs It was so obvious that they were attempting a handoff that I did not respond to her interests (This would be repeated a number of times in the coming months in other circumstances) She soon left and a man came in wearing a white T-shirt who had the Fed "look" I would run into him about two weeks later as I pulled off the interstate in Colorado to get a bite to eat

A couple more interesting anecdotes come from this same time frame While selling my books at Las Vegas, an environmentalist came up at the end of the show to look at my books I had just finished the chemical weapons book and he looked at it for a couple of minutes He then came up and asked me if I was some kind of a nut to put information like this out I told him not to worry as soon as someone takes a bunch of herbicide makes it into nerve

agent and wipes out a city, the government will take all the organophosphates off the market. It took a few seconds for the light bulb to finally go off in his head and then I saw him grin ear to ear and say "Yeah that would be good for the environment!"

On another occasion I called my dad from on the road and told him about the undercover hassles I was having. I also told him how I could tell the undercover agents apart by agencies in some cases. Our phone connection was crystal clear the entire time until I began to describe my observed differences in the FBI agents. The phone instantly began to crackle and we could barely hear each other. I told him I would call back later. [Details on this will be covered in the next chapter]

While in Houston, an individual came up, claimed he was a lawyer for the ACLU and asked me to call and talk to him about my case if I thought the government would try to arrest me for selling books. I was mildly suspicious and never called him. I would see him later at the end of the Great Western gun show and counted him as an agent which was obvious. [Lesson learned- the government fakes ID's just like criminals so don't believe anyone at their word or printed card alone.]

A pivotal point finally came at the Sioux City gun show in the spring of 1998. It would have a profound effect on my life and possibly the lives of many Americans. I had just completed and was selling my Chemical weapons book. An elderly nice old man came up to my table and started looking at my latest book. He had his young grandson with him and seemed very ordinary. He started to talk to me about the book's content and told me his son headed the army's chemical weapons program in Maryland. He wanted to set up a meeting between us and although I was leery I didn't want to offend him so I talked around it. He said "let me show you his picture with his family that I have here in my wallet." He opened the wallet to show me the picture and I glanced at it. I then noticed the blue imprint card with the emblem United States Central Intelligence Agency on the other side of his wallet. When he realized that was what I was looking at he immediately closed it and our conversation ended.

Later at Sioux City, after the show ended and I was packing up, another gun dealer from the show named Tom Brown came up to me. He and I and the janitors were the only ones left in the building and I was throwing my last boxes of books into my van. He told me that funny things happen to people who leave guns shows in the middle of the night. Vehicles come up behind them with their bright lights on at high speed and try to run you off the road. I told him I had never heard of that before and since I didn't have guns I doubted someone would be after my books that bad. He earnestly restated what he told me and it was obviously intended as a thinly veiled threat. I had

other veiled threats at other shows of a similar nature but nothing had ever happened so I didn't take it seriously

The next show at Sioux City took place in a couple of months and it was obvious this was not a normal show. One of the informants with the name of Andras Saleh worked very hard to establish a close relationship, buying \$400 worth of books, offering to buy a pizza after the show and talk about the info in the books and "other" things. He came up as the show ended and offered to help pack up and load my books. Then he asked if I was going home the same way I came to the show. I told him no as the alarm bells went off. I was also stupid enough to tell him my actual route. He then excused himself for a few minutes and went to talk to Tom Brown the same dealer that had made the veiled threat. I knew I had been had. I left with him with my guard up and ate the pizza, had the normal boring conversation with the exception of my book being compared to Adolf Hitler and then I left for home.

I took the route I said I would because I didn't think anyone working for the government would actually try to kill someone over a book they wrote. I also took one precaution. I sled my seat way back so that I was actually not in the window and was shielded by the panel in my van. As I pulled onto the Indian reservation north of Fremont, Nebr., a car pulled up rapidly behind me with its brights on. Then they pulled along side and I was sitting behind the panel and not in the window view when I saw a flash, then another bright flash. I thought they had shot at me but I heard no sound. I considered driving into their rear wheels to force them off the road but I peered around the corner and saw that it wasn't a gun but one of those large, million candle power strobe lights. They were trying to blind me. As they pulled in front and continued the light show I pulled my visor down to block it. Once in front, they pulled the strobe light in and as they set it on the seat it went off blinding them. They swerved all over the road and nearly ran off. I started to laugh even though the situation was actually quite serious. The Feds had sent the keystone cops to covertly kill me and very nearly ended up killing themselves. The aftermath would become much more serious.

The next morning my dad called and as usual asked me how the show went while getting me out of bed. I told him what happened and angrily said "for you assholes listening on the phone, I am going to describe how to make Malathion into nerve gas, and how to strap it to the mufflers of every secretary's car going into Washington DC. When the plastic melts they will gas the city. I'll teach that in my next book." This conversation took place on Monday morning. By Wednesday morning, as I left home to go eat, I noticed the several US Government license plates on cars that I passed on the way to the hiway. This did not go completely unnoticed since Silver Creek is a town of only 500 people. When I arrived at Pizza Hut in Columbus it was impossible to not notice the Lt. Colonel (Silver Oak Leaf on the collar) sitting next to my booth. He followed me back to Silver Creek and then back to

Columbus when I went for parts to repair my van. On the way back to my house I tried to pull window to window to talk to him but he pulled down the block. This was the first time the government sent the US Army out to babysit me. Unfortunately it would not be the last.

By the following Monday I had become incensed that they had done nothing about the undercover agents midnight activities so I called Andras Saleh (the informant) and confronted him over the phone about what had happened. He did not deny being a government informant and asked why I had not told him about this right away. In the course of our conversation I finally told him "Do you even realize what it is I know how to do, I could kill you with nothing more than a postcard in the mail coated with anthrax." At this point he finally cracked and I realized that he knew nothing of what they had set up. He was just being paid to do what they asked him to which was to try to make friends and delay my departure. I learned the lesson that in dealing with government snakes like this you can't even trust honest people because they use the honest ones to set up their dirty work. This would be a very valuable lesson in the years ahead.

In a humorous anecdote, some months later my landlords wife came over and told me her 4 year old son had gone out and told one of the men in the U S Gov't licensed cars that "Boy are you in trouble." The agent looked down at him and asked why to which he replied "My mom planted fresh grass there and you're parked on it." He then went to get mom. I explained to her that the government didn't like the books I wrote and became indignant that I would actually complain about their trying to kill me over them so they sent the agents out to babysit me.

I had actually tried to address what I would do if federal agents tried to arrest me for writing and selling books (especially in light of Ruby Ridge, Waco and the Oklahoma City bombing) and I decided that I would at least put up a creditable fight. When the US Army showed up outside my house I had these visions of Delta Force kicking in my door and arresting or killing me which I found almost unbelievable. Although my imagination and ego probably began to run away from me it was obvious that if the Army was coming I was really screwed. I felt I could deal in some surprising ways with law enforcement and it would all not go there way but I also knew from my military experience that I wouldn't stand a snowball's chance in hell if Army troops came to kick in the door. During all this I was enraged that they would send uniformed Army personnel to my home and not arrest their own agents for what was so obviously an illegal act. I finally concluded that the laws we live under no longer mattered and that I would have to contemplate the unthinkable.

I did not want to be arrested for writing books without at least a fight so the problem became how do you actually fight an army. The only way I could

conceive (at this time-I've improved since then) of a method was to build and equip my own army

Since Waco and Ruby Ridge as well as the advent of modern electronics combined with the real world army that the US Government was now willing to actually use against its citizens it was obvious that firearms, explosives and even chemical weapons would be practically useless. In my own particular instance I would be fighting nearly alone and would not be reinforced by anyone. This led to the creation of a new fighting concept which I would publish in my next book on biological weapons. At first I was practically horrified by the concept but after the way the Government had treated me and the way they made it extremely clear that my life and its laws were worthless to them, I got over the remorseful feelings quickly.

The core materials I published gradually, step by step, hoping the government would get the message and reform its laws or at least live by them. The only thing that would happen would be more dirty tricks. I consequently published where to find anthrax, plague, tularemia and dozens of other bacterial diseases, how to grow them on Jello and agar (in color pictures) and in soup. I included enhanced weapons designs such as mixing dermal irritants to anthrax so the targets would self-inoculate the organisms during exposure which would render the use of gas masks useless in a manner similar to that of mustard gas in WWI.

Finally, I published and simultaneously told the agents of my own army building concepts. In response to the obvious ability of the US Army or law enforcement to wipe me out, it would be possible for someone (acting on my behalf post mortem) with a big box of envelopes with anthrax under the postage stamps to send pre-addressed envelopes out to every hate group in America (or the NRA to rearm the country). Here is a ready-made army that hates the government already and that would actually fight if given invisible, self-reproducing weapons they could carry anywhere in the world undetected and grow overnight. Each of them could arm and equip their own mini-armies once they had the organisms and color pictures in the envelopes with some basic training instruction on how to safely grow and use them.

I completed my book on the bio weapons and in the months that followed widely distributed it. It soon became clear that the government had no conscience whatever and would not obey its own laws. In the summer of 1998, my book business was slowly dying with the summer gun shows, the harassment diminished somewhat and my anger and hate slowly melted away. I finally decided to try doing something else for a living but I would soon learn that the Government does not let people walk away so easily.

In the late fall of 1998 I began to sell computers. I borrowed the money from my parents and used sidewalk displays. Some of the wholesale suppliers had parts that failed, some would not ship key parts and computers for a

month and the business slowly died. Simultaneously, the undercover agents from the gun shows began to show up at my tables in front of HyVee. Some made intelligent conversation. Others made insults and threats. Others tried to talk about using the computers to link to anti government groups. It was the same o, same o. Just like a gun show every day.

The business quickly failed and I finally felt beaten and decided to try and find a regular job. After some difficulty I finally obtained work with Cummins tools in which we would setup truckload sales at different locations around the country each day.

My first day driving to the work site was illuminating. The crew boss was a former Army MP named Clint Hartung. I remained quiet and he slowly brought up gun show talk. It was clear that he had been briefed about me, a fact which he later did admit to but his real job was to sell tools and I found him in the next two weeks to be one of the hardest working and most decent men I have ever had the pleasure to know. I also realized that he was honest. There was no hint of evasion or deception whatsoever. When we finally had our serious conversation about his being talked to about me he told me he had been briefed and what did I expect considering the books I had written. He also told me that the incident at Sioux City was a warning rather than a murder attempt. If they had wanted to kill me they could have. I told him that my Biological weapons books were also a warning and that I could have easily killed many of them, but I didn't.

While selling the tools in Wisconsin, we had the gun show crowd once again deployed wherever I went. It was clear that I would never be left alone. I also had some difficulty getting in and out of the truck with my bad knees so at the end of the run I asked if I could sell tools on my own which is what I tried to do. A footnote to this trip included a conversation with one of the other crew members who was an obvious informant. He finally told me to my face that I would never be left alone. That I would never be left alone no matter where I went and what I did for the rest of my life. I remembered that conversation and it is the one thing that taught me that I would never take another job working for anyone else ever again.

In the spring of 1999 I decided to try my hand at selling tools. Once again the bulk of my daily contacts were the undercover agents. Now without witnesses around they began to use the insults again and in one case ran my customers off. They did this in front of a witness, my landlord who could identify one of them.

The business ultimately would fail. I was unable to finance advertising, vehicle repairs, inventory increases and tool trailer construction. The undercover agents also would begin to get on my nerves. I warned them that if they kept this up I would go back to the gun shows and convert my books to

CD's and sell them so everyone could afford them. From that moment on they poured it on. In addition to shoplifting a couple of one dollar items so that I would be sure to see it and then practically dare me to do something about it, they would show up to talk but not even buy the usual token items. This combination hastened my demise in this business and I sold what I had left and converted it to the computers and CD sales that you now see at the gun shows.

The 12 explosive, 3 incendiary, 3 booby traps, chemical biological and various other books that I sold for \$400 before. I could now sell for only \$20 and I also made the entire 5,700 page CD internet ready so that anyone could copy and send them anywhere on earth. It was my way of telling the government that it would not be allowed to do whatever it wanted to me and other citizens any longer without consequence. They may be able to harass or kill me which they regularly have threatened to do but my books will live on long after I am gone and will enable other people to fight back. I chose to fight with the words I could write. Others may not be so nice (I guess my problem in dealing with the government is that I haven't killed any of them yet-I must be too nice of a person)

One of the early shows on my return to the gun trade was at Belleville Illinois. At the start of this show a well dressed professional looking man came up and with some authority told me that Clinton had signed an executive order and that they were going to put a stop to my books. I told him they can arrest me whenever they feel like it.

Prior to this show and since then I have gone six straight months with \$1,000 in vehicle repairs. Some was no doubt required maintenance. Some had all the earmarks of direct sabotage. In five weeks I had to replace five tires. They were all worn to the inside. In addition all the rubber contact surfaces such as the windshield wipers, hoses, belts, front end steering guards were all eaten through in the same time frame. It appeared that Uncle Sam's agents had decided to use property damage as a means of stopping me from legally selling books. [I had considered publishing the use of rubber solvents that can be sprayed on the inside of tires to weaken the rubber and cause blowouts to the inside which is what happened repeatedly on my vehicle-(from assassination 101)]

While replacing my radiator in Little Rock, Ark. after the survival show there, a couple of the agents came in to strike up conversations with me. I finally decided to have some fun and when one of them commented to me that someone had shot at his vehicle and hit the bumper while he was driving through a bad neighborhood, I pined back that the shooter must have been a poor marksman if it was a deliberate attempt. He should have led your vehicle more. At that point the agent realized that I was playing with him, grinned and got up and left.

At Waterloo, Iowa one of the undercover agents came up dressed as a biker looked me square in the eye and said "when I kill people I like looking them in the eye" He caught me off guard but I soon replied that it would be kind of hard to do that when you're killing them a million at a time, wouldn't it

Several new approaches by the undercover bozos (I have by now demoted them from the status of agents to bozos) included trying to repeatedly get me to leave the country so they can just pay someone else to do the dirty work without having to explain it to anyone. I told them that isn't going to happen because if they intend to kill me they have to do it here where they have a chance of getting caught

Another one tried to pass off a phony \$50 bill and went out of his way to show me a printed roll of \$5 bills so I would catch on. This happened at the flea market in Nebraska City. I called the Sheriff and the undercover bozo who set up across from me came up and told me that no law enforcement officer at any level would be coming. I chased the individuals down the street who tried to pass off the bills so I could get their license number on their car but I was passed by another agent who sped down the hill told them I was coming and they left the area in the other direction. The message from this incident was obvious. they could pass phony bills and have me arrested when I tried to deposit them in the bank [and the sheriff never did show up]

Other incidents have included cars following me home in the middle of the night (after an evening out with my daughter at Columbus) with emergency flashers and brights on (they wouldn't pass). My computers in my house would behave funny and even the gauges on my car would act like yo yo's. When I would get angry and tell them I know you're listening and knock it off the odd events would cease. Its easy to see how they can do some of this. When I was in the U.S. Navy we would sometimes set up a prank by asking a new squadron member to carry light bulbs to the office across the hanger. When he passed in front of the APS radar on our plane we would turn it on and light up the bulbs he was carrying. We also regularly used our EW equipment to place phantom planes and ghosts on the radar scopes of Soviet planes and ships. They would chase our phantoms all over the oceans so it is easy to see how they can do this on computer screens. Playing electronic games is not new. In this case it is illegal and involves property damage and personal injury.

One interesting event occurred at the start of October 1999. I commented at a show that two women I recognized from a discovery channel program had been conducting surveillance on me in Columbus and I hadn't seen them in a few months. They were easily recognizable as a pair and I had noted their involvement in a U.S. Army program that had been highlighted on the show in which they placed electrodes in the brains of army volunteers to see how effective brainwashing might be using electronic methods. The women were interviewed on the program and I think they were CIA employees. My comments at the show were made on Sunday. The next day (Monday) at about noon as I was walking up

to the Columbus Wal Mart I noticed both women rushing up to meet me at the door. I ignored them and walked in. I wanted nothing to do with them.

At other shows bozos have come up in succession with comments about how police can gun you down by accident, or say they felt threatened, or how the wide open fields in the country here can be used to dispose of bodies so no one would ever find them. To that last comment I replied that perhaps the same can be said about Washington DC. Maybe centuries from now someone will be digging around on the East Coast and find the remains of a once great civilization and wonder what happened to it. It was at this time that I finally mentioned what I have known about for some time. I knew how to draft instructions for producing modified biologicals that could possibly depopulate virtually the entire planet.

The example I gave to the agents was a simple one. *Clostridium Perfringens* is the organism that causes gas gangrene. It is found in ox manure which the North Vietnamese dipped their punji sticks into to cause infected wounds in troops who step into the booby traps. We breathe this organism in and out every day. We eat it on our foods and it is found in our own solid waste. The reason it does not hurt us is that it cannot reproduce in the presence of oxygen. The spores only germinate in oxygen short environments like wounds with blood flow cut off and inside canned foods or underground in gardens.

If this organism is modified so it can become aerotolerant, facultatively anaerobic or aerobic it would likely wipe out every species on earth from the earthworm on up on the tree of life. I estimated the knowledge of how to do this was achieved around 1970 and the US Army almost certainly knew about it around that date. I could give thousands of other examples but this one alone should suffice.

One person in their basement could modify the organism and if only one ever gets out it would populate in the soil and spread. Whenever it was breathed in or swallowed by any upper life form it would produce toxins cutting off the flow of blood and immunity or other defenses and turning the tissues into food for itself (gas gangrene). There would be no defense and eventually it would spread across the planet eliminating everything that breathed it in or ate it. Now I wonder how powerful and arrogant the leaders in Washington feel now. They can't really do whatever they want anymore without consequence. I wonder if I have to write the next two or three books with all the procedures so everyone can do it. It's funny that a lot of people already know about this in this country. The government can't stop it.

All I ever wanted was to do my research work and take inventions to the marketplace. All I wanted from the government was fair laws so I could do so. All I have seen from the government is a succession of threats, harassment, attempted murder and contempt for their own laws. I have come to view the BATF, CIA, and even the FBI as paramilitary branches of the federal government.

I have vented my anger with my books and on some occasions with harsh invective and rancor towards the law enforcement officers or agents standing in front of me who in many cases likely do not understand why I am so angry. I am also sure the dirty tricks people do not announce to all their actions to those around them.

Ultimately, if this government does not do something about these people and live up to the promise of rule of law I am quite sure that one day someone is going to do it for them.

3. Differentiating General Public Behavior from HUMINT Collection

It is clear that undercover and related law enforcement practices involves not just catching criminals but in creating them as well (on both sides of the badge). A well informed public needs effective methods of identifying agents and activity in the field so they can protect themselves from these types of predators. In this chapter I will provide some of methods and techniques that have served me well in the field and at the gun shows.

In addition to the government practices and skills already described, a number of other habits and actions are required for undercover agents to do their job. The most important of these is recognition of their target. In order for an undercover operative to do their job they need to know who they are supposed to watch and create contact with. This gives the target a number of opportunities to identify agents from background populations and I will give a variety of field examples here in each case to provide some insight in how to identify them.

The first and most important skill is reading eye contact. When you walk through a mall or a Wal Mart store in a city where you have never been, watch how people look at you as they pass by. If you dress or look sharp they will notice you and some might make eye contact if attracted to you due to the context you created with the appearance. Do this with an ordinary or less than attractive appearance. Virtually everyone will not give you the slightest notice (context ordinary). If they look at you at all they appear to look through you at the items behind you or may appear daydreaming. Undercover agents who's job it is to watch and report will make or avoid eye contact in a manner in which they clearly recognize you. The only way they can use avoidance or recognition expressions is if they actually recognize you from being briefed.

If the agents job is to make contact, then they will attempt an eye appeal contact or smile to open a conversation. This must be taken into context again.

Are you dressed and groomed to deliberately create appeal. In your ordinary life, is this how others might approach you when they don't know you?

In the context of gun shows, I often left my shirt hanging out. Sometimes I would go a day without shaving and am overweight. I create a context in which there should be no interest whatsoever by women. After writing the chemical and biological weapons books I had a variety of approaches by women at the gun shows. Aside from the context of my appearance, the room was full of physically fit, single men who were far better candidates for their initial interest than I could ever be. It was obvious that the interest was artificial and generated by a government interested only in more dirty tricks.

Eye expression is useful when watching agents during their routine work. While working the shows they would look at books and literally "stare" through them. There was no real interest because they were not there as consumers to be interested in book and topical content. They were interested in the people buying the weapon books, or the gun transaction across the aisle, or were simply bored and trying to fill out their shift.

One other area useful as a test of a person's core belief system that I used at the shows involves the concepts of how to grow anthrax on jello, send it to all your friends and build your own armies. When I first stated this idea at a show, it shocked the initial listener. When you state it to ordinary people who are unaware of it, the response is one of shock, surprise, horror or very high interest depending on how the listener is initially inclined to accept the information. It would usually take a couple of seconds for their brains to interpret what you said and the light bulb to go off. Undercover people who have already heard about the concept do not find it new. In fact, if they hear it frequently they find it boring and this easily registers in their facial and eye expressions.

An outgrowth of this concept involves undercover bozos who come up to you and pretend to believe that the government needs to be overthrown and "we" should act to do something about this now. If they have not heard the idea stated above about the anthrax, they generally express surprise. Most were only superficially interested which indicated that their core beliefs were not anti-government but pro-arrest. An additional series of tests can be constructed to test these beliefs. By presenting fresh and insidious ideas like mixing anthrax and poison ivy together and mailing it to every employee of a particular agency you don't like (or secretly work for) you generate a response. Another example would be coating the mail with plague organisms on the outside of envelopes and saturating the target zip code so that every piece of mail becomes contaminated. If the person you are talking to understands these before he has seen you his eyes will remain dead or unmoved regardless of faked facial expressions and body language (translation-they are good actors). When you finally hit on a fresh concept that turns on a light bulb in their head their eyes give them away. The genuine anti-government consumers at gun shows generally find these ideas

useful and appealing. They are not interested in you personally like the agents are, they only want the information for themselves. If they find the concepts fresh and appealing, their pupils tend to dilate (become larger). If they are actually horrified or repulsed by the idea their pupils remain dead or more often contract in response to the suggestion. This is because the body responds to the brain's interpretation of frightening and horrific ideas. In this case the body's blood vessels constrict (blood runs cold) and you see part of this effect in the eyes (fight or flight response).

When you deal with genuinely angry people who are anti government and are inclined and prepared to fight them, they find new methods of fighting back appealing so the brain interprets this as something positive. Blood vessels dilate, the body relaxes and this results in dilation in the eyes. Sometimes you have to run a whole series of ideas past the undercover bozos to finally reach a fresh one they haven't heard so you can measure their response. Often they are so well briefed that they have heard everything and it becomes like talking to a dead fish.

Other common visual cues include -

Sincere smile = Creates wrinkles around the eyes

Fake smile = Creates no wrinkles

The test for this is what do they smile at that genuinely amuses them. This gives you a baseline to work from.

Anger = Eyebrows lower

Does the man genuinely become angry at the government or is he just faking it?

When a person is sad, eyebrows furrow which generate shadow (dark) areas higher on the face.

There are many books on body language and facial expressions which are useful in helping you determine if you are dealing with undercover agents or real people. These can help you ferret out the actors.

The most obvious way to tell people apart at gun shows and other situations is how they generally behave. The general public goes to the shows to buy guns, books, ammo and to occasionally socialize. The intelligence collectors try to mimic this behavior while acting to collect HUMINT (Human Intelligence). They tend to focus on behaviors that are primarily listening, moving to listening or filling their time till the shift ends. The public shops and comes or goes as they inclination suits them.

Another way of telling agents apart is the use of scripted conversation. They would come up with a preplan of "go up and talk to him about this". When they would do this the conversation would lose its spontaneity. This became so bad once at a show at Dallas that I finally told the young agent in front of me that one of the ways I tell agents apart from the public is their use of the scripted

conversation. He was focusing so hard on what he was supposed to say that he missed what I said. Another agent standing next to him did not miss it. We both grinned and he winked at me as he walked off.

Early on, the FBI sent in younger agents fresh out of Quantico to the shows. At that time they were notoriously easy to identify because they basically glowed with the persona that I have a badge, a gun, and I am super undercover cop. The older agents generally knew better. They had enough experience to know that bullets actually tear people up and that they were not bulletproof. The kids did not. This showed in their demeanor at the shows.

At a gun show in Novi, Michigan in 1998, I watched something being done by the undercover agents that I had not seen before. I noticed them moving in groups of 4-5 in paired formations two isles apart. I then noticed in the isle between them a uniformed member of the Michigan militia. Wherever he moved, they moved in parallel. When he stopped to talk, they stopped to "lean in" and listen in his direction from the isle away. It took him about 30 minutes to reach my tables and as he walked up I told him "you must be the most watched man at this show." At that instant the groups broke up and scattered every direction. I almost broke out laughing. He replied to me "let em watch, they know where to find me" and it was clear he was oblivious to the covert observation he was under. It reminded me of how overwhelmed and stupid I felt at the Minneapolis show when I first began to see the overall surveillance pattern.

Undercover operatives use a variety of electronics to assist them in listening to their targets without depending on agents. One of these is the use of ink pen bugs. These generally cannot be taken apart. When I first noticed parts of my conversations from my parents house and elsewhere showing up at the gun shows I realized that they were using bugs. I soon suspected and examined the free pens that I was being sent in the mail. I quickly learned to throw them out and the pens quit arriving. The listening continued however. I then realized that they would borrow my pen to use to write a check. Another agent would distract me and a bug would be placed in the pen which I then put back in my pocket. This allowed them to listen to every conversation I had at the shows. They could also switch pens. Even my car was repeatedly bugged. Once they were in such a rush to leave, they left the front pane. of my drivers seat on the floor with the screws off. I looked under the seat and talked directly into the bug and told them this must be the most bugged vehicle on the planet.

One advantage that they produced from this type of bugging is having the ability to find out what interests their target has so they can use it to brief agents to bring up the common interests or concerns. The van breakdowns were other examples. My watching certain TV programs repeatedly came up till I told them that was enough. You can use the DeJaVu from this to recognize agents. In real life they rarely come up as openers to conversations if ever. When the subjects are

broached in advance it is most likely a dead giveaway of a personal life briefing being used by an agent

One of the minor harassment techniques they also used involved a credit card company that I became annoyed with. Since they knew the Providence credit card company had annoyed me over a credit application they had the company send me weekly applications until I finally told them to knock it off because I was on to what they were doing. The weekly mailings abruptly ended then.

I also became annoyed and tired of having every single piece of mail I received opened and taped shut. They toned it down since I complained about this as well.

One of the techniques used lately by the agents who are apparently under pressure from Washington to get someone on the inside to do their dirty little frame up or other "law enforcement" job was to have the bozo (agent) step in front of me while I was browsing at books in a bookstore or walking into a Wal Mart. In order to use this technique they have to watch where they are going to see where to move to. This was easy to spot so I told them I knew what they were up to and they knocked it off. Shortly afterwards, they tried an "in your face" approach where they would have the agent move in close, chest to chest to invade my personal space. This didn't bother me since I knew what they were doing so they began to have uniformed police officers do it to crank up the intimidation level. The first time they did it they caught me off guard but I quickly realized what they were doing and this soon ended.

One final way of identifying agents is simply physical and voice recognition. You learn to recognize tattoos, hair color, identifying marks, speech patterns and so on. One of the most surprising visits at my table occurred when FBI director Louis Freeh stopped by. I didn't realize it at the time. All I thought was that he was someone used to giving orders so I figured he was one of the supervisors you regularly see. Some time later I was working on the computer at home and had a 20th century with Mike Wallace on the discovery channel on TV. I heard a voice I thought I recognized and I looked up at a special on law enforcement. The voice was the FBI directors and I realized that the big cheese himself had come out to visit me. For a few seconds I had this real intoxicating feeling of importance. Then the real world problems made me realize I needed to get my ego in check and go back to work.

A few final incidents that come to mind while writing this include the power being knocked out in my house (and not the neighbors) when I first tried to print out the chemical weapons book. The invasion of biting spiders when I was ready to print out the Bio Weapons book. The thinly veiled statements of dealers (agents) next to me at gun shows stating that "I had better hope I never lose my high profile."

4 Defense against Surveillance Practices (Counter Social Engineering)

“Biological and Chemical Weapons are like Lawyers. You need them to protect yourself against unjust Government, their horrible to think about, scare the hell out of you, and screw everything up if you ever have to use them!” Tim Tobiason

The US Government under which we live has adopted a number of policies and laws which seem best described as a by for and of itself form of governing

Personal observations and experiences have already been described and form a general pattern of –

- a A clear plan of framing citizens who write or say things it doesn't like
- b Institutionalizing the sciences of lying, deception and harassment
- c Sponsoring attempted murder and death threats

[In this regard I have often felt the US Government should put itself on the list of nations that sponsor domestic terrorism]

- d Having a policy of burning out armed resisters prior to Waco and then pretending that wasn't the case there
- e Massive surveillance of ordinary law abiding citizens

One other important comment I wish to make here is that there have been persistent rumors of the government building concentration camps (to which they will attach the less insidious name of internment camps). There is in fact indirect evidence of this and it can be contemplated in the following context

I have personally created the possibility of arming tens of thousands of angry citizens with the instant ability to create their own armies and wipe out cities. In the event a mass mailer delivers to tens of thousands of addresses in a single day such organisms as Anthrax or Botulinum and instructions on how to use them what would the government do. Anthrax can easily be mass produced and the spores hidden anywhere and stored for decades with the recipients being able to repeat what I have just described above at any time.

The only response would be for the Government to declare a state of emergency and start hauling people away to areas they can control them before everything starts to fall apart.

No amount of government electronic capability and individual force can cope with this genie out of the bottle for long. This will result in a quite drastic shift of power to private people and away from governments. The US Government would have to intern all individuals with anti government inclinations that they know about as well as all possible recipients to contain this threat. The only means of doing so then is the establishment of the actual infrastructure and plan of actions that have been rumored for some time.

I doubt the US Government would simply stand by and watch the overt arming of American citizens by this method and have presumed that they would adopt draconian and totalitarian practices in the name of preserving themselves (and Democracy?).

This author has developed a number of strategies and tactics that will enable the mass arming anyway. These include –

1. Teaching all Americans how to arm themselves with invisible, self reproducing weapons that each one of them can build and train their own armies with. I will be gone one day but I intend to insure that all people will have access to knowledge that will let them arm themselves against this kind of dishonest, power crazy and corrupt government. I am accomplishing this through the books I have written and distribute.
2. Arming millions of American citizens through third parties by means that I will describe in future books is another approach. One other approach is to simply publish the doomsday weapons procedures and let everyone have the singular ability to remove this government.

It sometimes seems that the people in Washington can write all the rules for themselves and their rich constituencies and the hell with everyone else. They need to learn how quickly their materially wealthy worlds can be brought to an end. I have made abundantly clear to the federal agents how easily Washington can be removed in a day (while they have made it abundantly clear how easily I can be removed in a day).

The US Government has adopted a social engineering approach of telling American citizens what laws it is going to have to live under or else. I have

adopted the opposite approach (counter social engineering) that we the citizens will have to tell the government what kind of laws we are going to live under and that these laws apply to the government as well and they have to be fair for everyone. This is a condition that certainly does not exist today. By using the internet to spread the knowledge of self arming and army building we the people should be able to stand up to any police force or army the U.S. Government sends against us.

As a practical matter there is no defense against determined surveillance by the Government with their ability to apply huge resources to any given area, person, or problem. This is why everyone needs to be armed with the knowledge and capabilities. They can't watch everyone all at once and cannot fight the entire population.

Once Washington realizes that it is functionally impossible to disarm the nation peacefully, and that it must reform or face a near certain civil war one day, perhaps they will decide to give in and live up to the promises of Democracy.

Instead of pretend Justice we can have real justice

Instead of pretend laws we can have real laws for everyone

Instead of pretend representation we will have real representation of all the people instead of just themselves

Instead of government by for and of itself we can have government writing and applying laws for everyone.

To those of you who will live on in this kind of world I wish you the best of luck. You do not have to be sheep and do whatever they tell you just because they can lock you up or kill you. You can fight back!

Postscript

Over the last two years, undercover agents would often follow an easily discerned pattern. They would feign interest in my books to get me up from sitting on a chair and then as soon as I would get up they would leave. As soon as I sat down, they would repeat the action. They would also do other things designed to create fatigue during the day. Near the end of the show day a new set of agents would come over. These would concentrate on using forceful techniques almost to the degree of bullying to create and reinforce hate for the President (if you hate him enough to threaten him you can be arrested), to believe in the oddball conspiracy theories and generally to reinforce the need for hating and taking action against the government.

The remaining undercover agents working the show are waved off to allow the Psy Ops people to work me over without interruption. This technique was intensified since the original publication of this book. I have estimated that about 20-40% of the dealers at the shows are agents or front men for the government and this allows them to effectively control the majority of the buying and selling of guns, gate receipts for the show promoters, traffic flow and overall intelligence collection. It has become obvious that Tim McVeigh would have been easily identified early on as an easy Psy Ops target and since he was young and had no training in being able to recognize what was going on around him he was obviously talked into retaliating. Whether the government knew he would blow up a building or not I could not say. Perhaps they simply thought that he would confide his plans to undercover agents so they could make another bust. Perhaps some of the players in Washington did in fact want to see a building blown up so they would receive more money for empire building.

Whatever the case, it is clear that the government uses techniques of exhaustion and forceful, sympathetic, and intellectual reinforcement in a planned and organized manner at the gun shows on certain targeted individuals to modify their beliefs and feed the hate. I personally believe that the government should not be in the business of paying people (agents) to brainwash American citizens into committing crimes for either arrest or empire building purposes. These techniques have been applied to me on and off for about two years and I have recently responded by telling the brain screw agents they send in that the only conspiracy going on at the gun shows is the use of agents to talk people into believing in conspiracies and basically (and politely) to buzz off.

Postscript 2

On 22 Oct. 1999 I drove to Minneapolis, Minn. I had bought a CD duplicator to mass produce the CD's I am selling (and you are reading). The duplicator would not duplicate any of the CD's and I wanted to find out why. It took about 30 minutes to realize that I had written the CD's in a form called packet data. The reason I had done this is that the Easy CD Creator program that had come with my Hewlett Packard CD Writer would not let me write the discs in the normal fashion. This occurred on all three of my computers so I used direct CD to bypass this problem. The technician at the company selling the CD duplicator began a series of tests to find out what was going on.

The first test showed that the easy CD Creator would not write any of my CD's files to a CD at all. I had originally believed this to be something called 'buffer underrun'. The technician advised that this was not the case. We ran a second test. This

time we used files that were not my own STIP CD's but were other data files on the computer. This test was successful every time. The CD Writer had no problem in taking other data and making it into duplicatable CD's.

We decided to run one last test. If the computer could not copy my own data then there was a problem with the way I was writing my data. The technician installed the same Easy CD Creator software on my computer but carefully placed in a different directory. This time we tried to create 'normal' master CD's on my computer. This time it worked. I then told the tech that my other computers were exactly like the first and could he please install the same software on my other machines. The look I received from him was very funny.

For those readers who are unfamiliar with computers, I will enlighten you.

1. When a person such as myself goes to the store and buys a CD writer, he receives a software package that lets the user write CD's in what is called a standard format. This is done with every writer and computer sold in the world without difficulty. In all three cases of my 3 computers and 3 writers this was not the case. None of them would write a properly formatted CD. I ended up using a method that would write what is called packet data. This method leaves the front end formatting data off the CD making it physically impossible for anyone to copy my CD's in a CD duplicator but would still allow anyone with a computer to read the data. The net effect of this would be to prevent anyone with a CD duplicator from buying my CD's and mass producing them by the thousands.

2. In my computers case, it would copy all the other data on my computer except for my own STIP files (on all three computers).

3. When we installed the same software to tell the CD writer how to write the CD's in a different directory, it would then copy my own files correctly which means that it was not a problem with my file types.

The reader can make their own conclusions from this story with the following anecdotes.

- A) At the Belleville show I had been warned that Clinton had signed an executive order and that "they" were going to put a stop to my book crap.
- B) At the Hamburg New York show, I was distracted by a customer and turned away from my computers. A girl working the booth across from me with her father came over and asked if she could play on my computer like the other woman was. As I turned around, the woman on my computer bolted in one direction while the man distracting me bolted the other direction. I didn't try to stop them because I didn't know what they had done. From this moment on, my computer would not write CD's anymore. What had happened is that they had changed the read speed on the computer from 24X to 2X so that when it would proofread at the end of the writing, it would take about an hour instead of 2-3 minutes and appeared that the machine had stopped.

The US Government is obviously paying its agents to covertly interfere with the free press (STIP) thereby subverting the 1st amendment that they clearly don't believe in. I just thought you the reader would like to know

Tim Tobiason

Postscript 3 7 March 2000

I am including several new observations of the undercover agents activity around me and my interpretation of it.

1. During this winter I traveled to Portland Oregon for a 1400 table gun show. While in the parking lot of a gas station south of Portland I was "burning" sets of CD's three at a time in preparation for the show. The CD duplicator reliably kicked out three CD's at a time from my master. Several agents pulled into the parking lot (from the gun shows). Almost immediately, the duplicator would quit and start beeping indicating that all the CD's were bad. Prior to this my failure rate was about 1%. After consulting with the manufacturer, they told me that the data stream to the CD's had to be interrupted in order for all three to go bad. I moved away from the agents to another parking lot without agents parked next to me and the CD's were produced perfectly using the same master and the same spindle of blanks.

At the Little Rock show a few weeks later (New Years Weekend) I was producing CD's before the other dealers came in. I commented to one setting up next to me who I knew was undercover and trying hard to warm up that my CD's were running OK and at least no one was destroying them. Almost from that moment on and until Saturday night, every CD I attempted to make was bad. The agents, whose purchases and entry fees to the shows account for most of the commerce at the shows bought almost no product leaving me with a tiny fraction of my normal sales. By Saturday at 4 PM I had decided to leave the show without finishing on Sunday. Shortly after telling the show promoter I was planning to leave, another agent showed up and told me that since I was having such a tough time at the shows that maybe he could find a job for me locally, perhaps working at a lab. I told him no. Then he asked if I would be interested in going to work for the government. I was so angry by now that I told him "after the attempted murder, army outside my house, weekly dirty tricks and the deliberate property damage that I would rather commit suicide and kill a bunch of agents before I would go to work for the government."

2. At the above mentioned Portland show which I went into angry over the damage to my CD's, I went through a 10 hour stretch of no sales.

During this period, I counted 7,000 people walking by and could positively identify over 5,000 of them from gun shows in Nebraska and east. These were people I had personally talked to. I interpreted this as a demonstration by the "Feds" of their ability to control and limit the commerce of any individuals they wished at the shows. If I would tell someone that the government indirectly ran and financed every gun show in America it would scarcely be believable. It is certainly a testable hypothesis and based on these observations I have concluded that gun shows will be preserved in America by law enforcement as a direct means of observing gun sales and anti government individuals that they can then target for arrest, harassment, and psychological operations

- 3 As has often happened in the past, my phone conversations have turned up at the gun shows. Before a recent show at Council Bluffs, Iowa, I had a phone conversation at my parents house with the IRS. I owed them a small amount of money in back taxes and had made an agreement to pay them. I even commented to my parents that the undercover agents will probably now work me over on this at the show this weekend. Sure as clockwork, the agents went to work. One pair wanted to do my taxes. Others strongly promoted not paying taxes and others to not even file. In the previous year I had the tax conversation come up perhaps once. I purposely avoided the subject since I knew that it would be broached first by the obvious undercover agents. In one case I even correctly picked out the agent coming up to me as one of the "Brainscrew" operators and I was right on the money.
- 4 I have seen occasions where then agents have covered for their agent dealers by catching gun thieves before they could leave the show. I have estimated that 15-35% of all the dealers at the shows are working for the government in one capacity or another. There have been some instances where guns have been stolen at the shows without the thief being caught. I have concluded that this is almost impossible given the density and habits of the agents unless they are the ones doing the stealing. This is also easily testable by methods I will not publish here.
- 5 The following letter was received by me from a reporter in Kansas and is self explanatory. The public defender involved wanted to represent me if I was arrested in Kansas. He was evidently hired by the FBI to do this and assist them in arresting and convicting me in court. It is interesting that the FBI is more interested in rewarding their agents who concocted this scheme rather than firing them for obviously encouraging illegal actions. This is consistent with my impression of the government law enforcement arms being para criminal branches of the federal government.

JOURNAL-WORLD

Dolph C. Simmons, Jr.
Editor in Chief

ESTABLISHED 1891

Ralph Gage
General Manager

Scientific and Technical Intelligence Press
Box 59
Silver Creek, Nebraska 68663

Feb 14, 2000

Dear Mr. Tobiason,

My name is Dave Ranney. I'm a reporter with the Lawrence (Kansas) Journal-World.

I'm in the process of writing a story about Dan Rupp, a former investigator with the federal public defender's office in Wichita who was fired, he says, because he cooperated with the FBI in an investigation of your activities. Mr. Rupp and others allege that, in short, you are dangerous.

My story will focus on the lawsuit Mr. Rupp has filed in an effort to get back his job, but I do need and want to give you the opportunity to respond to the aforementioned allegation, i.e. Are you dangerous? Do your activities pose a threat to the nation's security?

With this mind, please call me at Journal-World 1-800-578-8748 during normal business hours. I'm at extension 7222. I'm usually there until about 7 p.m. If I'm not at my desk, please leave a message.

Thank you,

Dave Ranney

Dave Ranney

Filed at K.C., Mo. Rupp vs. US Publ. Def. Office

To Whom it may concern

From Timothy W Tobiason

PO Box 59

Silver Creek, Nebr 68663

308-773-8278

www.stupid@hotmail.com

I am sending this letter to several news media in the hope that one of you will pick this up and report it. For over two years I have written and sold books that our government has deemed dangerous and I have been targeted to force an end to publication. The enclosed book on "Undercover activities and agents" chronicles my experiences of the last two years.

In early 1998, a man handed me his card at a gun show and indicated he would like to be involved in representing me if I am arrested over the sale of my books. He was an employee of the public defenders office. He was also wearing a wire and working for the FBI. He was fired for doing this and in a subsequent lawsuit the judge ruled in effect that he could not do this and retain his job.

His deposition and those of the FBI agents is enclosed along with the judge's ruling. Many statements were attributed to me at the shows which formed the basis of their actions and, although they sound completely crazy, I will be the first to admit they are completely accurate. Except for one tiny additional detail that they left out. Prior to writing the books on biological weapons and their undercover activities, I had been warned and threatened at the shows and an attempt was made to blind me with a strobe light and run me off the road. I wrote these books after this incident. At every gun show afterward and including my conversations with Mr. Rupp (the Public Defender's office) I stated this was the reason for my writing the books and making threats regarding the government. I did this in as loud and obnoxious manner that I possibly could.

The depositions make no mention of this at all. They even chose to not use the tape recording from the wire as this would have been self incriminating. At a later show I got into an argument with who I presumed to be an FBI supervisor and told him that when we land in court all those tape recordings are going to be subpoenaed and they would have to explain them. He told me that all those tapes can easily disappear to which I replied "that only works if you have the only copies".

I am not a nice person in many peoples eyes. What I do for my living is well explained and legal. We live under a government that does not recognize the laws that we live under and evidently can do whatever it wants to us in the middle of the night and get away with it.

I have enclosed the "Undercover agent" book, a CD containing all the background material on the biological and chemical weapons referred to in court, and copies of the court depositions and judges ruling. This is at the very least a newsworthy story that will undoubtedly eventually make headlines. If you are interested in pursuing this you may contact me at the above address and #.

Thanks

Tim Tobiason



20 Paul W. Vick - 8/16/99 3:41 PM

Rupp vs. Phillips

Page 1 to Page 55

CONDENSED TRANSCRIPT AND CONCORDANCE
PREPARED BY:

AAA REPORTING COMPANY
101 West 11th Street, Suite 1010
Kansas City, MO 64105
Phone: (816) 471-2766
FAX: (816) 471-4995

EXHIBIT A

Page 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

AMEL RUPP,
Plaintiff,

Case No. 89-2103-WEA

DAVID J. PHILLIPS, in his
personal capacity,

Defendant.

VICENATED DEPOSITION OF PAUL W. VICK, a
witness, taken on behalf of the Plaintiff, pursuant
to Subpoena, on the 16th day of August, 1989, at the
United States Department of Justice, District of
Kansas, 100 State Avenue, Suite 160, Kansas City,
Kansas, before

MYLES A. HEGGE,

for AAA Reporting Company, a Registered Professional
Reporter, Certified in Kansas and Missouri.

APPEARANCES

For the Plaintiff

MR. LEE J. HOLLIS
THE HOLLIS LAW FIRM, PA
5100 West 95th Street, 2nd Floor
Peculiar Village, Kansas 66207

For the Defendant:

MR. DOROTHY DAVID FISCHER
HUSCO & EPPENBERGER, LLC
301 North Main, Suite 250
Wichita Kansas 67202

Page 2

APPEARANCES (Continued)

For the witness:

MR. JANICE MILLER KARLIN
ASSISTANT UNITED STATES ATTORNEY
UNITED STATES DEPARTMENT OF JUSTICE
500 State Avenue, Suite 160
Kansas City, Kansas 66101

Also present

Mr. Dan Rupp
Mr. Kevin Seach

THREE

WITNESS	PAUL W. VICK	PAGE:
Examination by Mr. Hollis		3
Examination by Mr. Fischer		31
Re-examination by Mr. Hollis		48
Re-examination by Mr. Fischer		49

EXHIBITS:	MARKED:
1 - Report	3
2 - Letter from Rupp to Tobiasen	3
3 - Reply from Tobiasen to Rupp	3

Page 3

(The deposition commenced at 10:41
a.m.)

(Deposition Exhibit Nos. 1 through 3
were marked for identification.)

MS. KARLIN: For the record, we have
already indicated on the transcript for the
deposition of Resident Agent William Seck that
this deposition is governed by three
authorization letters which are included as part
of Deposition Exhibit 4.

PAUL W. VICK,

a witness, being first duly sworn, testified
under oath as follows:

EXAMINATION BY MR. HOLLIS:

Q. Could you please state your name for the record?

A. Paul W. Vick, V-i-c-k.

Q. Mr. Vick, you are an FBI agent?

A. Yes, I am.

Q. And you currently reside in Wichita?

A. Yes.

Q. How long have you worked in the Wichita office?

A. A little over three years.

Q. Can you trace your history with the FBI for the
Court and the jury, please?

A. Yes. Well, I was a detective on the Wichita

Page 4

police department, quit in Wichita, Kansas from
the department in December of '83, and I joined
the FBI in April of '84 and was hired to go to
Quantico, Virginia and then I went from there to
the San Diego division for four years. Then I
went to New York City for four years, went back
to California for another four, San Diego
division. Then I came to Wichita, Kansas and
I'm working on my 16th year in the bureau.

Q. All right. And are you currently anticipating
any career moves coming up?

A. Yes. In May — on the 26th of May I took a
promotion, supervisory special agent position,
in Washington and I'll be leaving there at the
end of this week, leaving Wichita to go work in
the Washington area.

Q. And what is your exact title or what was it as
of the summer of 1988?

A. Special agent.

Q. How did you come to meet Dan Rupp?

A. I had the fine occasion of dealing with Mr. Rupp
on a couple criminal cases where as a FBI agent
investigating criminal cases in the Wichita
area, I was — on occasion had to go to court,
and on one occasion I took two defendants to

Page 5

1 trial in Wichita, and during the course of that
2 case, Mr. Rupp was assisting federal defenders
3 and I got to know him that way either before the
4 trial or during the trial, and then for a period
5 of time after that on occasion his office -- he
6 in particular would deal with our office on --
7 certain cases in the normal course of their
8 office defending people that we were --
9 investigating.
10 Q. What would his involvement be in the normal
11 course of defending cases, Mr. Rupp's?
12 A. I didn't deal necessarily directly with Dan, but
13 I think -- in trying to set a background on how
14 I met Dan and I don't remember the exact day.
15 It was a particular trial. But after meeting
16 Dan -- we're in the same Epic Center building at
17 301 North Main, and I would see Dan coming and
18 going from the parking lot on the fourth floor
19 where our office is. So just coming and going,
20 I would see Dan on a personal basis. But aside
21 from that, I don't remember any specific cases
22 where our office had to deal with their office,
23 but I think that there were a few
24 Q. Okay. Just can't remember the specifics?
25 A. Yeah.

Page 6

1 Q. When do you first recall meeting or discussing
2 with Mr. Rupp the Timothy Tobiasson situation?
3 A. June the 8th of 1998.
4 Q. Okay. And as part of your job as an FBI special
5 agent, did you compile reports of your
6 activities?
7 A. Yes.
8 Q. And I'm going to show you what's been marked as
9 Exhibit 1 in front of you. Is that the report
10 that's been -- and your attorney has taken a
11 black magic marker and marked out parts of it
12 that they don't want to reveal for statutory
13 purposes, but other than that, is that your
14 report that you made in connection with your
15 conversations with Mr. Dan Rupp?
16 A. Yes.
17 MR. FISCHER: Lee, do you have
18 another copy of those?
19 MR. HOLLIS: I don't.
20 MR. FISCHER: Okay.
21 MR. HOLLIS: I mean, I've got one
22 copy, but I need to refer to it.
23 MR. FISCHER: Okay.
24 If I could just take a look at it
25 before he starts to ask questions.

1 MS. KARLIN: We'd be -- also be happy
2 to make you a copy
3 MR. FISCHER: That would be fine if
4 that's okay.
5 MR. HOLLIS: Okay. Let's go off the
6 record
7 (Discussion off the record)
8 Q. (By Mr. Hollis) Okay. We're back on the
9 record. Now, was Exhibit 1 a report that you
10 prepared at or near the time of the subjects
11 that you wrote about?
12 A. Yes. If I could just --
13 Q. Okay.
14 A. -- finish answering your first question as far
15 as that this document documents my conversations
16 with Mr. Rupp. Sometimes we in the FBI get
17 accused of being a one-way street, but this does
18 not reflect my conversations with Dan Rupp. It
19 reflects information that he gave me with --
20 Q. Okay.
21 A. -- regards to his contact with someone that we
22 had an interest in
23 Q. Okay.
24 A. So I just want to clarify that because --
25 Q. Okay

Page 8

1 A -- it doesn't document any verbal things that I
2 told Dan.
3 Q. All right.
4 A. So I'll --
5 Q. Okay
6 A. -- try my best today to remember if you ask me
7 questions about --
8 Q. Okay.
9 A. -- conversations.
10 Q. Going back to Exhibit 1, when you wrote the
11 report, you were writing about conversations you
12 had with Dan Rupp and that's what's in the
13 report; correct?
14 A. Yes.
15 Q. And it was the regular practice of you as an FBI
16 special agent to maintain reports like that of
17 sources that you talked with?
18 A. Yes.
19 Q. And it was in the course of the regularly
20 conducted FBI activity that you kept it?
21 A. Yes.
22 Q. And were you the custodian of that document?
23 A. Of the original?
24 Q. Or of -- yes
25 A. No, the original goes in an informant file that

Page 9

we have in our office in Kansas City.
But you were the person who wrote it?
Yes, sir.
Okay.

MR. HOLLIS: Move for admission of
Exhibit 1 as a business record. Do you have no
objection?

MR. FISCHER: No objection.

Q. (By Mr. Hollis) How did you come to talk with
Dan Rupp on June the 8th? And tell me what you
recall was said.

A. I don't keep notes with regards to exactly what
I say to people that give us information. If I
can recall, Dan came down to our office on the
fourth floor to give information to me with
regards to a concern that he had with regards to
someone that he met for the second time at a gun
show in Wichita on June the 6th. It was the
second meeting that he had with this individual,
having met this person a year before that. And
I'm not -- I can't tell you whether or not Dan
would have provided the same information to any
other agent in our office. All I know is -- I
don't know why Dan came to me other than we had
kind of a cordial relationship passing in the

Page 10

hallways over a period of time. Anyway, if I
remember right, he had some information and I
invited him in the office and we discussed the
information he provided me on that date.

Q. Okay. And what information did Mr. Rupp provide
you on June the -- what day was it?

A. June the 8th.

Q. 8th.

A. Do you want me to basically read the document
that he -- I mean, how do you want me to -- just
in general?

Q. Well, did Mr. Rupp tell you that he attended a
gun show?

A. Yes.

Q. And what did he tell you about who he met at the
gun show and what he found out?

A. He told me that he met an individual at the gun
show who had a lot of documents for sale that
had to do with chemical and biological weapons.
He spoke with this individual and -- Dan did --
and the individual made comments that he had a
surprise for federal agents that were -- if they
tried to arrest him or search his property, he
had a -- it seemed that he had a hostility
towards federal agents that he thought were

Page 11

following him. And because of the threat issue
with regards to the federal agents maybe getting
hurt or killed and because of some of the
chemical and biological information that this
gentleman had in verbal conversations with Dan
Rupp and also in writing, Dan felt that it was a
real concern to the public that he disseminate
this information to us on that date. So --

Q. And what was your feeling about that?

A. I appreciated getting the information. I didn't
have really any feelings other than documenting
the information that he gave me and I was
appreciative of the information that he gave.
With me also knowing the kind of job that he had
with the federal defender's office, we did not
want to put him at risk with regard to his job.
We did discuss options on how he could be of
further help to us. I do believe we discussed
the option of being a cooperating witness
where -- that's a term that we use where a
person can be used to testify later. That
person may volunteer to be wired up and discuss
things with a person that we have an interest
in. And that would then necessitate the person
eventually having to testify. Dan, if I

Page 12

remember right, told me on the day that he
provided the information to us that he did tell
his boss or bosses about the fact that he was
coming to our office with this information, and
at the time I don't believe that his office had
a concern with regards to him initially
disseminating this information to us, but they
did ask him not to become further involved with
regards to having to testify because it would be
a conflict of interest. So we -- our office
honored that request. We have a lot of people
that provide information to us in the private
and business sector, and we open people up as a
confidential source to document information such
as Dan provided us and we had the intention of
using additional information that he would
provide to us on a confidential basis and it
would be written up in such a way that he would
not be identified and that he would not have to
testify in court. And so we felt comfortable
with that information or at least that
relationship, that if he had any additional
information of a real serious threat with
regards to this same individual, that we would
appreciate his continuing to provide that kind

Page 13

1 of information to us.

2 Q. What's the difference between a cooperating

3 witness and a confidential source?

4 A. A confidential source is someone, like I said,

5 that just — that provides us information and

6 their identity is protected. That person is

7 given protection by our office from disclosure.

8 A cooperating witness is someone that may be a

9 person that has come to us that is in trouble

10 criminally and has information about an

11 associate and for whatever motivation reasons,

12 the cooperating witness will go further to help

13 us than a criminal informant or cooperat — I

14 use the words interchangeably. A confidential

15 source and a criminal informant are pretty much

16 the same. A cooperating witness is a person

17 then that would agree to testify in court and

18 would not object to wearing a body wire and

19 taking a further — more overt acts which would

20 cause that person to have to testify later on in

21 court.

22 Q. When you met on June 6th, what did Mr. Rupp say

23 about Tobiason's experiments?

24 A. On June 8 you mean?

25 Q. June 8th.

Page 14

1 A. Yeah. With regards to his experiments?

2 Q. Right.

3 A. He was told — Mr. Rupp was told that this

4 individual was using toxic biological chemicals,

5 and he specifically mentioned some kind of a

6 Jell-O which he would grow in a medium-like

7 toxic material. He also discussed using

8 malathion or parathion, using ultraviolet lights

9 to switch the ionic charges in the chemicals to

10 turn the substance into a nerve gas and he

11 discussed some other things.

12 Q. And did Mr. — did he say what Mr. Tobiason said

13 about what would happen if any agents came after

14 him?

15 A. He mentioned that he was going to have a

16 surprise for the agents. He also made some

17 comments about that it's not going to be

18 pretty. It seemed to — by the way Dan was

19 telling the story to me of his conversation with

20 this individual, that the person had intentions

21 of harming federal agents or, in addition to

22 that, killing civilians as a result of whatever

23 he was working on.

24 Q. And did Mr. Rupp talk about what Tobiason had

25 said about how to get anthrax and the history of

1 anthrax?

2 A. Yes.

3 Q. What is anthrax, by the way?

4 A. Well, I personally am not a chemist. I think

5 anthrax, the chemical name is b-a-c-i-l-l-u-s

6 anthracis, a-n-t-h-r-a-c-e-s. It's — they're

7 ingredients from nature which can be used to

8 form bacteria that can be real bad. It's very

9 toxic to humans and it can kill people if it's

10 inhaled or ingested.

11 Q. Was there another gun show then scheduled for

12 the weekend of June the 13th?

13 A. I believe so, yes.

14 Q. And was there some indication that Mr. Tobiason

15 might be there?

16 A. Yes.

17 Q. And did you later learn whether or not he showed

18 up?

19 A. I believe that Dan told me that he did not see

20 him on that day at the gun show in Wichita.

21 Q. And then did you at some point either on or

22 after June the 8th ask Mr. Rupp to write a

23 letter to Mr. Tobiason?

24 A. I'm not real sure with — my recollection is —

25 how that conversation came up. All I can

Page 15

1 remember is that there was a relationship

2 established between Mr. Rupp and Tobiason, and

3 because of that relationship, I did encourage

4 Dan to continue the dialogue with Mr. Tobiason

5 and if he wasn't showing up at a gun show, I

6 thought that by his — I'm trying to get to the

7 question as to — I'm not sure if I told him to

8 write it or if we just discussed it and Dan

9 didn't have a problem with it or if it was Dan's

10 idea. I'm not sure exactly how that — the —

11 that came up, but, nonetheless, I did encourage

12 him, yes, to send a letter to Mr. Tobiason.

13 Q. And what was your understanding of Mr. Rupp's

14 background with Mr. Tobiason in terms of when he

15 had first met him and what they had discussed at

16 that time?

17 A. I'm not sure that Dan had a close relationship

18 with this person, but I know that a year before

19 at a gun show Dan had met this individual and

20 had conversations with him and was a little

21 concerned I think at that time a year ago, a

22 year previous to that June of '98, that this

23 individual had some similar interests with

24 regards to just weapons and general chemistry

25 conversations. And so when he met him then

Page 17

again in June of '98, he renewed the -- I don't know, the relationship that he briefly developed the year before, so...

And Mr. Seck, your supervisor, testified that he believed that a public safety issue was involved here. Do you agree with that?

A. Yes.

Q. Why?

A. Just from the information that Dan gave me that came from the lips of this individual and from some of the written materials that the individual had which were later provided to me by Dan, and any comments about the fact that we're following him or that -- and that he's hostile towards federal agents and he intends to have -- he has a surprise for them and in the same context he's talked about how many people could die if -- if he followed through with these ideas of chemical and biological agents that he was experimenting with, that there was a possibility that people could die, federal agents could get hurt or killed, and so I did think it was a safety issue.

Q. Did you have him under surveillance otherwise?

MS. KARLIN: Objection. This is

Page 18

outside the scope of his authorization.

Q. (By Mr. Hollis) Your lawyer won't let you answer that question then?

A. I'd feel uncomfortable answering that question at this time.

Q. Because it's outside the scope of --

A. Yes.

Q. -- what you're allowed to testify to?

A. Yes.

Q. So there was a discussion of -- well, Mr. Tobiason failed to show up for the June 13th gun show and then you discussed with Dan how to reach him. Did he have a telephone number?

A. This individual deals with an address. His literature has an address, like a PO box in Nebraska -- well, in the United States, and I don't believe that there was a phone number associated with -- with this individual. There may have been, but I think that we only discussed the possibility of Dan sending a letter to the PO box.

Q. And why did you want -- why were you encouraging that that be done?

A. I was hoping that this individual would continue to provide Mr. Rupp with, if not his intentions,

Page 19

if people were going to get harmed, I was hoping to find out any additional information that this person might be -- might have that he would be providing Mr. Rupp, and also perhaps the schedule that -- of the gun shows that he's going to attend in the future, and also the -- I know that Dan had a real concern about that this gentleman may carry out these threats, and so Dan wanted to basically tell the guy not to follow through with any of these threats. So he was actually trying to, in my opinion, diffuse the situation by encouraging this guy not to carry through with some of the threats that he had heard him make.

Q. And is Exhibit No. 2 a copy of the letter that Dan Rupp wrote to Mr. Tobiason?

A. Yes.

Q. And the note at the bottom, that was something that Mr. Rupp included. Was that at your suggestion or his idea or do you remember?

A. I don't recall whose idea it was, to be honest with you. The comment about please advise when you may be at this town again and please do not act until we talk, I believe that Dan came up with that idea as far as his concerns that this

Page 20

guy not act. So that -- that may have been Dan's.

Q. Okay. And then is Exhibit 3 a copy of the response and the accompanying envelope that came back to Mr. Rupp?

A. Yes.

Q. And can you read what Mr. Tobiason wrote at the bottom of Exhibit 3?

A. "Dan, I have already decided an effective and quite appropriate solution to both the justice system and government's actions. Thanks anyway."

Q. And below that?

A. "Be at Wichita 13" -- "11 to 13 September" -- "Be at Wichita show 11-13 September?"

Q. Okay. And can you tell -- tell us when you talked with Dan about this response letter, Exhibit No. 3, and what you recall of those conversations? In fact, if you can just tell us what you recall of any conversation that you had with Mr. Rupp from June the 8th onward. I know you told us about the first conversation on June the 8th. Then you had another conversation with him sometime after June the 13th where you talked about writing a letter, correct?

1 A. Yes.

2 Q Were there any conversations in between June the

3 8th and June the 13th or June the 14th?

4 A I do know that on the 29th -- are you asking

5 between that time frame?

6 Q. We'll get to the 29th. But first of all, just

7 to make sure we haven't missed anything, were

8 there any conversations that you had with

9 Mr. Rupp after June the 8th and --

10 A. I don't recall.

11 Q. -- and before the letter was written other than

12 what you've told us?

13 A. I don't recall.

14 Q. Okay. And after the letter was written, what

15 conversations do you remember having with

16 Mr. Rupp?

17 A. I did make a -- document a conversation I had

18 with Mr. Rupp on the 29th of June with regards

19 to the letter, and I believe the letter was sent

20 out on or about the 16th of June. And then he

21 received a response back from this individual on

22 the 29th of June. And it was postmarked I

23 believe the 25th of June

24 Q. And with respect to the note "Be at Wichita

25 show 11-13 September?" at that point did you ask

1 A. If I could just make a comment. One of -- I

2 noted later that one of the reports that you

3 have, on the bottom it gives the date of the

4 investigation, and this is a report that starts

5 out saying that Mr. Rupp was contacted on

6 September the 12th. At the bottom I've got

7 7/11 -- or 7/12 of '98. That's a typo. That

8 should be 9/12 of '98, September.

9 Q. Okay. When you talked with Mr. Rupp on June the

10 29th, are you saying you can't recall any

11 conversations between June the 29th and

12 September the 12th with Mr. Rupp?

13 A. I don't recall speaking with him, but if you

14 have some information that you could help me

15 with with regards to refreshing my memory, I'd

16 be happy to -- I don't recall the specific

17 dates.

18 Q. Did you ever go to the public defender office to

19 talk with Mr. Rupp on this subject?

20 A. I believe that I did go up to their office on at

21 least one occasion to communicate with him, yes.

22 Q. Which occasion was that? Do you recall?

23 A. I don't remember

24 Q. Was there more than one occasion when you went

25 to the public defender office to talk with

1 Dan to go to the show and check on -- see what

2 else he was up to?

3 A. I don't recall directing Dan to go to the

4 shows. Knowing the job that he had, I do know

5 that he -- Dan has an interest in firearms and I

6 think he was a private investigator previously

7 and he on his own as a civilian has an interest

8 in doing whatever he likes to do, attending

9 these gun shows or whatever. I just asked Dan

10 that if he did have an occasion to go to these

11 shows and if he saw this individual and had

12 conversations with him, I would of course be

13 very happy to know what this individual told

14 him. And so, anyway, I didn't direct him to go

15 to the show. Dan I believe went on his own.

16 Q. Did you have any conversations with Mr. Rupp

17 between June the 29th and the middle of --

18 and -- well, after June the 29th, what

19 conversations can you recall having with

20 Mr. Rupp?

21 A. I believe I had conversations with Mr. Rupp on

22 the 12th and the 13th of September

23 Q. And --

24 A. And --

25 Q. Go ahead.

1 Mr. Rupp about this subject of Mr. Tobiason?

2 A. I don't believe so. I -- I'm not trying to be

3 evasive. I'm just trying to recall. In fact,

4 I don't even know if I ever went up there to

5 have him contact me. Usually when we develop a

6 relationship with someone that's providing us

7 information, we try to -- I know that I told Dan

8 to keep it quiet that we were helping him -- I

9 mean that he was providing us information just

10 because we like to protect anybody that's

11 providing us information. So because I've had

12 dealings with their office before, it's not

13 unusual for me to go up there and just say,

14 "Hey, could you have Dan contact me?" But

15 generally, these meetings were set up -- I'd

16 either get a phone call from Dan or he'd just

17 stop in the office if he had information. So I

18 honestly can't remember if I went up there

19 specifically with regards to this issue.

20 Q. But you asked Mr. Rupp to keep confidential your

21 dealings with him?

22 A. Yes. This is after the first day that he

23 provided us the information on the 8th of June

24 Q. And after the September -- what did you talk

25 with Mr. Rupp about in September?

Page 26

On the 12th of September, Dan had another meeting with this individual and there was a conversation that I was -- I mean, Dan Rupp told me that the source told him that he, the source -- I mean -- excuse me. The source was surprised to -- there was a quote, surprised to see you, and this individual responded, I'm not dead yet or in jail. That was one comment. And in the same meeting on the 12th of September, that individual stated that federal agents were still messing with me, bothering him, following him, and wanting to talk to him. The government was sending people in to get close to him, but that individual knew that they were agents. These were conversations that he had with Dan Rupp.

Q. And did Dan Rupp say that Mr. Tobiason had a story to tell about his complaints with respect to his problems with the government?

A. Yes.

Q. And what did Mr. Rupp say Tobiason said about getting his story out?

A. I can't remember if it was that day or the following day when the individual said that -- what do I have to do, kill a million people, or

Page 26

I forget the number of people that he was talking about killing to get attention to his cause. Oh, I see. It was on the 12th of September, referring to this report. "I'm not afraid to die. I'm ready to fight. What do I have to do, kill a million people, to get them to print my story?"

Q. Then did you talk with Mr. Rupp again on September the 13th?

A. Yes.

Q. And what did Mr. Rupp say that Mr. Tobiason said when Rupp asked, "See you" -- or said, "See you next year"?

A. Mr. Rupp heard -- well, this individual told Mr. Rupp, quote, I'm not going to be around afterwards to deal with any consequences. The government has gone too far and someone needs to stop them and I'm going to stop them. He made some other comments such as, "It's too late for that." When -- when Dan I think was trying to diffuse the situation, initially the gentleman told Dan, "You won't see me next year. You're going to read about it in the news. They've gone too far and it's too late for that," with regards to Mr. Rupp trying to get this guy to

Page 27

change his mind. So it seemed pretty ominous, the information that was coming out from this individual.

Q. And what did Mr. Tobiason say about his delivery methods?

A. He seemed to talk as though he had some expertise or experience in this area and he said -- he stated that he can send the plague virus around in the mail or I don't even have to use the mail. I can put ethyl -- ethylene oxide, which was a gas, through the pipes into any building, even into the White House. He didn't personally threaten the life of the President, but he used the security of the White House as an example of how he could get -- could target locations. He did not mention using explosives or nerve gases -- nerve agents or biological agents at that time, but he talked about putting this gas or interjecting gas into the White House.

Q. What did he say about viruses?

MR. FISCHER: I'm just going to object here. This is getting into some hearsay because you're asking him what Tobiason said as opposed to what Rupp told him Tobiason said

Page 28

Q. (By Mr. Hollis) What did Rupp say Tobiason said about viruses?

A. I'm not sure

Q. I think it's 7/13, page 2, or 9/13.

A. Oh, Mr. Rupp was told that this individual was making viruses. That was something that Dan Rupp was convinced of just from the way that he talked and he indicated that he may even have some of these viruses in his van out in the parking lot.

Q. And what did he say in conclusion, Mr. Rupp say that Mr. Tobiason said in conclusion?

A. He stated that sometime in the past, government agents whom he assumed were National Security Agent agents spoke with him and asked him what he wanted in order to -- to get this person to stop putting out this type of material. And this is the written materials that he disseminates all over the place when he goes to these conferences. The individual was telling Dan that he wanted the patent laws changed to make it more fair for individuals like himself to obtain patents. He acted like he had come up with some ideas or patents that weren't getting approved and he seemed to be real disgruntled

Page 29

1 over that issue. He concluded on that
2 particular meeting that Mr. Rupp would not be
3 seeing him again and that the book business
4 wasn't working out financially and he ended up
5 by saying that he was going to, quote, fight
6 them. Someone has to and I'm going to do it.
7 Q. And these notes are taken in connection with
8 your investigation of Mr. Tobiason?

9 MS. KARLIN: Objection. I think
10 that's outside the scope of the authorization.
11 Q. (By Mr. Hollis) Your lawyer won't let you
12 answer that?

13 A. Yes.
14 Q. Was the situation with Mr. Tobiason an apparent
15 emergency?

16 MS. KARLIN: Objection. The
17 authorization letter talks about conversations
18 between Mr. Rupp and this agent. I have allowed
19 him to go a little bit just by way of
20 background, but I'm not going to let him talk
21 about whether the FBI felt it was an imminent
22 threat, a natural disaster. I think he's gone
23 as far as we really should allow.

24 MR. HOLLIS: Okay. Well --

25 MR. FISCHER: I also want to object

1 both. If a person just develops a virus or
2 something that's harmful, if it's not coupled
3 with a threat or an actual act or an attempt --
4 you know, some kind of a threat or an action,
5 it's not against the law.

6 Q. Was Dan Rupp ever employed by the FBI?

7 A. No, he was not.

8 Q. Did he ever work undercover?

9 A. No, he did not.

10 Q. Was Mr. Tobiason considered dangerous?

11 MS. KARLIN: Objection. It's outside
12 the scope of the authorization and he is not to
13 testify.

14 Q. (By Mr. Hollis) Did you have any other
15 activities planned for Dan Rupp or was the
16 September gun show the last thing that you had
17 in mind for him to do?

18 MS. KARLIN: Objection, outside the
19 scope of the authorization. I instruct him not
20 to testify.

21 MR. HOLLIS: I think I have no further
22 questions at this time.

23 EXAMINATION BY MR. FISCHER:

24 Q. Agent Vick, my name's Dwight Fischer. I'm here
25 on behalf of Dave Phillips, federal public

Page 30

1 that it calls for speculation.

2 MR. HOLLIS: I'm just going to ask a
3 few questions and if you want to instruct him
4 not to answer, that's fine.

5 Q. (By Mr. Hollis) Did the FBI have anyone in a
6 better position to do what Dan was doing in
7 terms of contacting him than Dan?

8 MS. KARLIN: Objection, outside the
9 scope of the authorization.

10 MR. HOLLIS: Instructing him not to
11 answer?

12 MS. KARLIN: I am.

13 Q. (By Mr. Hollis) Was there other information
14 about activities that Tobiason had been involved
15 in that you had possession of other than what
16 Dan Rupp had told you about?

17 MS. KARLIN: Objection, it's outside
18 the scope of the authorization and I instruct
19 him not to testify.

20 Q. (By Mr. Hollis) Is it a federal crime to
21 develop and threaten the use of weapons of mass
22 destruction?

23 A. It's a federal crime to generate biological
24 agents and then use them to threaten or kill or
25 harm people. It has to be a combination of

1 defender, who's the defendant in this case. Is
2 it your understanding from your conversations
3 with Mr. Rupp that Mr. Tobiason displayed these
4 manuals that he produced, that he displayed them
5 in public at these gun shows?

6 A. Yes.

7 Q. And that he discussed them in public?

8 A. Yes.

9 Q. And that they were for sale in public places?

10 A. Yes.

11 Q. And that he even went so far as to market these
12 materials, correct?

13 A. Materials that did not talk about threatening
14 federal agents and killing people, but materials
15 that told people how to make these various types
16 of chemical or biological agents, yes.

17 Q. And materials that would be cause for concern?

18 A. They're scientific materials which caused
19 concern when I looked at them, but they're -- if
20 you're in the scientific industry or -- it's
21 kind of how-to type books. Selling them at a
22 gun show to people that just come there, normal
23 citizens, I would think a normal citizen would
24 be concerned about those materials and there
25 were concerns. There.

Page 33

Q. you had no reason to think that he was producing these manuals in secret; he was public about these manuals —

Yes.

Q. — correct?

A. Yes.

Q. Based on what you said before, Mr. Rupp served as a confidential source; is that what you referred to him as? Is that correct?

A. Yes.

Q. And that's something that you use from time to time in the FBI; correct? He wasn't the first one you've ever had?

A. Correct.

Q. You also discussed how there's a distinction between a cooperat — or a confidential source and a cooperative witness; correct?

A. Yes.

Q. Is there any time that a confidential source becomes a witness without being cooperative?

A. Repeat the question. Is there a time — if I understand it right —

Q. Let me rephrase it. Is it always up to the confidential source whether or not they will be used as a witness?

Page 34

A. No, it's not. And I'll just give you a brief example. If —

Q. I don't need a brief example. That's fine

A. Okay.

Q. Did Mr. Rupp ever ask you to be compensated for the information he was providing you?

A. Absolutely not. The only compensation, if I remember, was two instances where I reimbursed Mr. Rupp either 20 or \$30 for the purchase of these manuals. I felt that we needed to reimburse him for that.

Q. At times informants are compensated though; correct?

A. Yes.

Q. With a confidential source such as Mr. Rupp — well, let's just talk about Mr. Rupp specifically. You directed him to keep the information that you shared between the two of you confidential; correct?

A. Yes.

Q. From whom was he supposed to keep that confidential?

A. I asked him to keep it confidential from anybody.

Q. Including his employer?

Page 35

75009

A. I didn't specifically say who he should not talk about, but I just told him that if he was going to provide us information, it would be best — we tell all of our sources to keep it confidential from everyone that they're providing information to us.

Q. And everyone would include his employer; correct?

A. Yes.

Q. Did Mr. Rupp — you can finish taking your notes. Did Mr. Rupp — and you discussed this before. I just want to clarify. Was it your understanding that before he came and spoke with you, Mr. Rupp had told his employer that he was going to be providing this information to you?

A. I can't remember if — if he told his employer after he provided the information, just to give them a heads up, that he received some real serious information that he thought was serious that he did turn over to us, and I believe that — I can't remember if he got — if he told his employer right before or right after I believe it was right after, at which time then his employer gave him some parameters on not becoming involved any further to where he would

Page 36

have to become a witness and some other things like that.

Q. Who discussed those conversations with you? Did Mr. Rupp tell you that he told his employer this and that his employer gave him the parameters?

A. Yes.

Q. You never discussed this with his employer?

A. No.

Q. Did Mr. Rupp ever talk to you over the telephone or in person during regular business hours?

A. I believe so, yes.

Q. Meaning Monday through Friday?

A. Not always. If something came up where he had — where he met with Mr. Tobiason, he would get in touch with me on the weekend. If he received some information, he would disseminate that to me fairly quickly. So I'm not sure exactly what day of the week these contacts were on, but I think some of the contacts were during business hours.

Q. Meaning Monday through Friday, approximately eight to five, there may have been times when you met with him —

A. There may have been, yes.

Q. — or spoke with him during those times;

Page 37

- 1 correct?
- 2 A. Yes.
- 3 Q. Mr. Rupp told you that Mr. Tobiason had said
- 4 that he thought he had been contacted by agents
- 5 of the National Security Agency previously?
- 6 A. That's what he told Mr. Rupp.
- 7 Q. So based on what Mr. Rupp told you, Mr. Rupp had
- 8 reason to believe that government agents had
- 9 previously contacted Mr. Tobiason; correct?
- 10 A. All I can tell you is what Dan told me, and with
- 11 regards to this individual telling Dan that he
- 12 had been contacted, he was a very paranoid
- 13 individual and thought that he had been
- 14 contacted by undercover agents or people with
- 15 National Security. Whether that happened or
- 16 not, I'm not in a position to say at this point.
- 17 Q. Through the time of your September 12th and 13
- 18 meetings, 1998 meetings with Mr. Rupp, during
- 19 those meetings or at any time beforehand, did
- 20 you discuss with him additional contacts you
- 21 would like to have him made with Mr. Tobiason?
- 22 Did you ever discuss the possibility of this
- 23 continuing in the future?
- 24 A. Yes.
- 25 Q. Did you discuss any specifics with him in terms

Page 38

- 1 of specific contacts you wanted him to have with
- 2 Mr. Tobiason in the future?
- 3 A. No, I think that each time I met with him or
- 4 that he gave me information, I just thanked him
- 5 for the information and encouraged him to
- 6 continue the contact with this individual.
- 7 Q. Did you ever give him specific directions of
- 8 contact to make?
- 9 A. Other than discussing this letter to see what
- 10 kind of a response it would generate back, I
- 11 don't remember telling him anything other than
- 12 what he was going to do really in his private
- 13 time on weekends going to these gun shows as a
- 14 private citizen, not on company time, you might
- 15 say, and if he came across more information that
- 16 we'd be interested in, I encouraged him to
- 17 continue to provide us with that information.
- 18 Q. And in terms of the letter, you said before you
- 19 couldn't recall whether it was your idea or
- 20 whether it was Mr. Rupp's idea to generate the
- 21 letter; correct?
- 22 A. I can't remember at this point.
- 23 Q. When you met with him or spoke with him in
- 24 September the 12th and 13th of 1998, had there
- 25 been any arrangements made for you to meet with

- 1 Mr. Rupp again in the future or was it just left
- 2 open generally, let me know what you hear?
- 3 A. I think that it was left open with regards to
- 4 him contacting me if he came across positive
- 5 information. That could have been a year from
- 6 now if he bumped into this gentleman again.
- 7 Q. But it was your understanding that there was the
- 8 likelihood that you would have additional
- 9 contact with Mr. Rupp regarding Mr. Tobiason;
- 10 correct?
- 11 A. Well, not after the last conversations that
- 12 Mr. Rupp had with this individual. It seemed
- 13 that something horrendous or something was going
- 14 to happen which was going to cause him not to be
- 15 around much longer. So it was kind of up in the
- 16 air.
- 17 Q. But it was your understanding that if contact
- 18 did occur, that Mr. Rupp would be letting you
- 19 know about it; correct?
- 20 A. Well, I encouraged him to disseminate
- 21 information back to us if he had positive
- 22 information.
- 23 Q. You previously discussed the fact that you had
- 24 met Mr. Rupp at some criminal trials or a
- 25 criminal trial; is that correct?

Page 40

- 1 A. Yes.
- 2 Q. What was your role in that trial?
- 3 A. I was the case agent.
- 4 Q. Meaning that you investigated the individual
- 5 that was on trial?
- 6 A. Yes, individuals.
- 7 Q. And for whom were those investigations
- 8 conducted?
- 9 A. What do you mean, for whom?
- 10 Q. They were on behalf of the U.S. attorney?
- 11 A. Yes.
- 12 Q. And you're aware that Mr. Rupp is an
- 13 investigator; correct?
- 14 A. Yes.
- 15 Q. Are you aware of who he investigated for?
- 16 A. Yes.
- 17 Q. And who did he do investigations for?
- 18 A. Are you talking specifically on this one trial
- 19 or --
- 20 Q. As an employment -- during the time you had this
- 21 relationship with him or this contact with him.
- 22 A. For the federal -- federal public defenders.
- 23 Q. Are you familiar with what the role of the
- 24 federal public defender is?
- 25 A. Yes.

Page 41

What is it, in your understanding?

They provide legal assistance to defendants that are charged that can't otherwise afford a private attorney.

Q. And these are individuals oftentimes who the FBI has investigated on behalf of the U.S. attorney?

A. Yes.

Q. And the U.S. attorney is prosecuting these individuals; correct?

A. Yes.

Q. And the federal public defender is charged with defending the individuals; correct?

A. Yes.

Q. So oftentimes or generally you're on opposing sides from the federal --

A. Yes.

Q. -- public defender, correct?

A. Yes.

Q. Did it ever cross your mind that Mr. Tobiason may at some point be defended by the federal public defender?

A. I'm not real sure if I gave it much thought, to be honest with you. I'm not sure how to answer that.

Q. Is Mr. Tobiason the type of person that the

Page 42

federal public defender defends?

MR. HOLLIS: Objection, calls for speculation.

Q. (By Mr. Fischer) Is Mr. Rupp continuing assisting you in investigations in any way at the present time?

MS. KARLIN: Objection. I'm not going to object if the question is as to the individual that he was previously -- who has been previously identified as Tobiason, but because the question is broader than that, it is outside the scope of the authorization.

Q. (By Mr. Fischer) Is Mr. Rupp continuing to assist you in your investigation with Mr. Tobiason?

A. Since Mr. Rupp's employment was terminated with the federal public defender, I think that there have been a contact or two with regards to some follow-up with regards to this individual.

Q. Can you tell me about those conversations?

A. I don't recall specifically what -- what they were about.

Q. Were they conversations that you initiated or that Mr. Rupp --

A. I don't think that -- that I initiated -- the

Page 43

agreement, if you want to call it that -- and keep in mind that the whole time that Dan was providing this information to me and to our agency, I was very, very mindful of the fact that -- of who he worked for. And because of that, we tried to stay within the parameters of not compromising his employment.

Q. Okay. I don't mean to interrupt, but I'm right, now questioning you about things that have occurred since he was no longer employed.

A. I was trying to get to the point of the fact that more than likely it was just Dan reporting to me by phone or whatever that he had another contact with this individual or that he went to a gun show and didn't see that individual at a gun show.

Q. Okay.

A. That would be pretty much the other follow-up with regards to this particular criminal case.

Q. Okay. I'd just like to move to strike that as nonresponsive and just ask you, have -- are you saying that he's just given you follow-up telephone conversations since he's been terminated by the federal public -- since he -- let me strike that. Since he's no longer been

Page 44

employed by the federal public defender's office, it's your testimony that he has contacted you in regard to Mr. Tobiason?

A. Yes. That's not the only thing that we would discuss, however, in these subsequent meetings.

Q. Well, what else would you discuss?

(Discussion off the record.)

A. It mostly had to do with the demise, his demise you might call it, with regards to your office and proceeding with plans that he had to believe try to get his job back. And so they had to do with dealing with a lawyer or lawyers and information that he was trying to get from us that may be helpful in his case.

Q. (By Mr. Hollis) And what information was that that he was attempting to get from you?

A. I believe reports that would document at least the contacts that he had with our office, something that could be helpful to him later on.

Q. And those are the reports that have been used --

A. Yes.

Q. -- as exhibits today --

A. Yes.

Q. -- correct? Have you done any investigation of Mr. Tobiason that did not involve Mr. Rupp?

Page 46

1 MS KARLIN: Objection, outside the
2 scope of the authorization.
3 Q. (By Mr. Fischer) And so you're not going to
4 answer because of the instructions of your
5 attorney; correct?
6 A. Yes.
7 Q. Do you feel the FBI was capable of investigating
8 Mr. Tobiason without the assistance of Mr. Rupp?
9 MS KARLIN: Objection. It's outside
10 the scope, instruct him not to testify.
11 A. Prefer not to answer that.
12 Q. (By Mr. Fischer) The FBI is a government
13 agency; correct?
14 A. Yes.
15 Q. And you have offices throughout the United
16 States; correct?
17 A. Yes.
18 Q. Approximately how many full-time employees does
19 the FBI have? Do you know?
20 A. 27,000, I think.
21 Q. And offices throughout the United States?
22 A. Around the world, yes.
23 Q. Around the world. Do you have any idea what the
24 FBI's annual budget is?
25 A. I would not want to make a guess, but it's in

Page 46

1 the billions.
2 Q. And going back to your discussion of Mr. Rupp
3 being a — what did the CS stand for?
4 Confidential —
5 A. — source.
6 Q. Confidential source. He's not the only
7 confidential source you've ever used; correct?
8 A. No.
9 Q. During your first conversation with Mr. Rupp,
10 you testified previously that you discussed the
11 possibility of there being problems with his
12 employer regarding his role in assisting you;
13 correct?
14 A. I don't think that we used it in the context of
15 problems, but I do know that Dan spoke with me
16 with regards to the federal public defender's
17 concerns that Dan not be a witness and that
18 there may be a conflict of interest, and so we
19 were real careful about not receiving any
20 information from him on any — anything that
21 your office was doing other than him reporting
22 these pretty minimal contacts with this
23 individual that we had an interest in.
24 Q. So at the beginning of this contact with
25 Mr. Rupp, you were aware that his employer

1 potentially had concerns about his involvement
2 with you?
3 A. At the end of the first day that he provided the
4 information to us, yes, I did know.
5 Q. And based on that, you still instructed him to
6 keep any information he had confidential from
7 his employer; correct?
8 A. Only within the parameters of your office, the
9 federal public defender's office, not wanting
10 him to ever be a witness. And we — the whole
11 case that we had with regards to Dan providing
12 us information was kept in that context. He
13 would never have been a witness.
14 Q. Okay. I'm just going to move to strike that as
15 nonresponsive. Let me rephrase my question.
16 Knowing that you did that his employer
17 potentially had concerns about his involvement
18 in this investigation, even knowing that, you
19 told him to keep his involvement confidential
20 from everyone; correct?
21 A. Yes.
22 Q. And as you've said before, everyone would
23 include his employer; correct?
24 A. Yes.
25 MR FISCHER: I have no further

Page 46

1 questions.
2 REEXAMINATION BY MR. HOLLIS.
3 Q. I have just a few follow-up questions. First of
4 all, was it possible in your mind that Mr. Rupp
5 would become a witness in the Tobiason case?
6 MR. FISCHER: I'm going to object.
7 That calls for speculation.
8 Q. (By Mr. Hollis) You can go ahead. And I'm just
9 asking the question that Mr. — you answered a
10 few moments ago that Mr. Fischer asked to be
11 stricken from the record. What was your thought
12 about the likelihood of Mr. Rupp becoming a
13 witness in the Tobiason case?
14 A. Zero.
15 Q. In all of the conversations that you had with
16 Mr. Rupp through the summer and fall of 1998
17 about Mr. Tobiason, did Mr. Rupp ever talk about
18 any other cases that the federal public defender
19 was working on?
20 A. No.
21 Q. Did you ever ask him about any other cases that
22 the federal public defender was working on?
23 A. No.
24 Q. Were you working on a murder case called the
25 Lisa Dunn case where someone named Lisa Dunn was

Page 40

charged with murder?

MS. KARLIN: Objection. I'm not going to allow him to testify what other cases he was working on.

Q (By Mr. Hollis) Well, let me ask you this: I think this is within the scope of the parameter. During any time that you talked with Mr. Rupp, did he ever talk to you about anything with respect to the Lisa Dunn murder case?

A. No.

MR. HOLLIS: Thank you. No further questions.

REEXAMINATION BY MR. FISCHER:

Q. I just have a couple follow-up questions. Why do you say that there was zero chance that Mr. Rupp would be a witness regarding Mr. Tobiason?

A. Because that's the framework in which the agreement that we made on the first day he provided us the information was set up. I've had cases in the past where you just make a decision early on to honor commitments or desires. And the whole time that I was dealing with Mr. Rupp, knowing his position and the fact that he was doing this on his own private time

Page 50

on the weekends or whatever, it really didn't concern your office with regards to the information he was providing. And so I did not want to create a conflict by having to testify and so we were honoring that and at no time did I from probably the first day on intend to use him as a witness. The first day, I will say though, before we found out about these parameters and the comments from your office, the federal public defender's office, I had -- I mean, the first thing that an investigator wants would be, hey, shoot, let's wire them up. Let's see what we can get on tape. But once we found out that your office had a problem with any kind of witness information, we decided to honor that and I feel that we did do that.

Q. Was that information relayed to the federal public defender?

A. My boss attempted to sit down with Mr. Phillips and explain the difference if he had a question as the difference between a cooperating witness and a confidential source, and it's my understanding that Mr. Phillips declined to meet with my boss on that matter.

Q. Are you aware that that proposed meeting

Page 51

occurred approximately 3 1/2 months after your contact with Mr. Rupp initiated?

MR. HOLLIS: Go ahead.

A. Yes.

Q. (By Mr. Fischer) So at no time in the intervening time between June 8th and September 23rd did anyone from your office attempt to explain that to the federal public defender, is that correct?

A. No, because we didn't have a need to do that.

Q. From the FBI's perspective, you had no need to do that, correct?

A. Yes.

Q. So based on your involvement with Mr. Rupp in this investigation -- let me strike that. Based on the arrangement that you made with Mr. Rupp at the beginning of his involvement with this investigation, you were proceeding under the assumption that you would be able to continue with any investigation and potential prosecution of Mr. Tobiason without the assistance of Mr. Rupp?

A. Yes.

Q. Therefore, he wasn't vital to the prosecution of Mr. Tobiason?

Page 52

A. By -- I'm struggling with --

Q. I'll withdraw the question.

A. -- with the vital part.

Q. I'll withdraw the question.

MR. FISCHER: Nothing further.

MR. HOLLIS: Nothing further.

(The deposition concluded at 11:50 a.m.)

CERTIFICATE 21-1-21

Myles A. Megee
Certified Shorthand Reporter
State of Kansas

MAM

1
William R. Seck - 8/16/99

Rupp vs. Phillips

Page 1 to Page 12

CONDENSED TRANSCRIPT AND CONCORDANCE
PREPARED BY

AAA REPORTING COMPANY
101 West 11th Street, Suite 1010
Kansas City, MO 64105
Phone: (816) 471-2766
FAX: (816) 471-4995

EXHIBIT C

Page 1

Page 2

Page 3

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

AMIEL RUPP,
Plaintiff,

Case No. 99-2301-MCA

DAVID J. PHILLIPS, in his
personal capacity,

Defendant.

VIDEOTAPED DEPOSITION OF WILLIAM R. SECK, a
witness, taken on behalf of the Plaintiff, pursuant
to Subpoena, on the 16th day of August, 1999, at the
United States Department of Justice, District of
Kansas, 500 State Avenue, Suite 360, Kansas City,
Kansas, before

MYLES A. HOLLIS,

for AAA Reporting Company, a Registered Professional
Reporter, Certified in Kansas and Missouri

APPEARANCES

For the Plaintiff:

MR. LEE J. HOLLIS
THE HOLLIS LAW FIRM, PA
5100 West 95th Street, 2nd Floor
Prairie Village, Kansas 66207

For the Defendant:

MR. ONIGHT DAVID FISCHER
RUSCH & OPPENBERGER, LLC
303 North Main, Suite 350
Wichita, Kansas 67202

Page 2

Page 4

APPEARANCES (Continued)

For the witness:

MS. JANICE MILLER KARLIN
ASSISTANT UNITED STATES ATTORNEY
UNITED STATES DEPARTMENT OF JUSTICE
500 State Avenue, Suite 360
Kansas City, Kansas 66201

Also present:

Mr. Dan Rupp
Mr. Marvin Seck

THREE

WITNESS WILLIAM R. SECK PAGE:
Examination by Mr. Hollis 3
Examination by Mr. Fischer 4

EXHIBITS MARKED:
- 8/16/99 and 7/19/99 letters from Motegor to
Hollis and 8/16/99 letter from Williams to
Hollis 3

(The deposition commenced at 10:29
a.m.)

(Deposition Exhibit No. 4 was marked
for identification.)

WILLIAM R. SECK,
a witness, being first duly sworn, testified
under oath as follows:

EXAMINATION BY MR. HOLLIS:

Q. Could you please state your name for the record?
Oh, I'm sorry, your attorney wants to
say something first.

MS. KARLIN: Do you want me to be on
the camera or just - I don't care how it works,
but -

MR. HOLLIS: I think it's just on the
witness.

MS. KARLIN: Janice Miller Karlin
appears on behalf of the witness, Supervisory
Senior Resident Agent William Seck. This
deposition is being conducted pursuant to an
authorization for testimony that has been given
by the Department of Justice under the
provisions of 28 CFR Section 16.22(a). Marked
as Deposition Exhibit 4 to this deposition and
to the deposition of Special Agent Paul Vick are

three authorization letters. The first letter
is dated June 18, 1998 for - I'm sorry, '99,
for Special Agent Vick, the second is a letter
authorizing the limited testimony of Agent Seck,
and the third is a letter dated today's date
which supplements or is an addendum to the prior
two authorization letters. And this witness and
Agent Vick will be allowed only to testify in
accordance with the authorization and not
outside of that authorization.

Q. (By Mr. Hollis) Okay. Could you please state
your name for the record?

A. I'm William, middle initial's R, last name
Seck, S-e-c-k.

Q. And you are an FBI agent?

A. That is correct.

Q. You office out of Wichita?

A. Yes, sir.

Q. And what's your relationship with Agent Vick?

A. I am his immediate supervisor.

Q. Okay. Did you work with Agent Vick in the
summer of 1998?

A. Yes, I did.

Q. And you were familiar with his investigation
which involved communicating with Dan Rupp?

1 A. Yes, sir.

2 Q. And did you have occasion to talk with David
3 Phillips at any point in time with respect to
4 Mr Rupp?

5 A. Yes, sir, I did.

6 Q. And how many conversations did you have?

7 A. One, as I recall.

8 Q. Can you tell me what you recall that you said
9 and he said in that conversation and what was --
10 who called who?

11 A. I called him.

12 Q. And what was the purpose of the call?

13 A. The purpose of the call was to -- in an effort
14 to have a face-to-face meeting with him when it
15 became apparent to me that there was some maybe
16 perceived difficulties, the fact that Mr Rupp I
17 guess had run into problems with his -- with his
18 own agency because of his cooperation with the
19 FBI, and I just thought it would be appropriate
20 to broach him and see if he would like to meet
21 face-to-face.

22 Q. Can you tell us, the Court and the jury, what
23 you recall Mr -- you said and Mr Phillips said
24 when you talked with him when you called him?
25 And when was the conversation?

1 A. My recollection was September 23rd of 1998.

2 Q. Okay Can you tell the Court and the jury what
3 was said by you and by him?

4 A. I called him. I identified myself. I don't
5 think I had met him previously. I identified
6 myself, told him that the reason I was calling
7 was because the word had got to me as a
8 supervisor that there were some -- there may be
9 some problems because of Mr. Rupp's cooperation
10 in our investigation. I recall telling him
11 that -- that we believe the information was
12 important, that we were appreciative of Mr Rupp
13 coming forward with that information.

14 Q. What information?

15 A. Just the information he was providing regarding
16 Mr. Tobiason, you know, could have a public
17 safety issue involved, that we were concerned,
18 and that if he was concerned that Mr Rupp would
19 be acting in capacity of doing something
20 operational, that being wearing a wire or some
21 kind of body recorder, was not an issue because
22 we had only opened him up as a cooperating
23 source or informant and such in that capacity we
24 would not be asking him to do those things, only
25 provide information. That's really all I recall

1 about the conversation. It was apparent that
2 Mr Phillips really didn't want to discuss it
3 over the phone and really wasn't interested in
4 meeting me in person. He was very cordial. He
5 was very professional. He listened patiently
6 and I probably repeated my story maybe one more
7 time and it was thanks, but no thanks, and the
8 conversation ended.

9 Q. And what had Dan Rupp done with respect to the
10 investigation of Mr Tobiason that you refer to
11 that you felt implicated a public safety issue?

12 A. Well, I don't know if I'm comfortable answering
13 that. Because of the scope of my conversation
14 with Mr Phillips over the phone, it was my
15 understanding this is what I would be talking
16 about here this morning.

17 MS. KARLIN: For the record, the
18 authorization only allows Mr. Seck to testify
19 about the information that he provided to
20 Defendant Phillips and the information that
21 Mr Phillips provided back to him.

22 MR. HOLLIS: Okay Well, with that
23 restrict on in mind, I have no further
24 questions

25 And if you want to ask some questions,

1 I can let you come over here.

2 MR. FISCHER: I can probably do it
3 from here.

4 MR. HOLLIS: Okay

5 THE WITNESS: Okay.

6 EXAMINATION BY MR. FISCHER.

7 Q. I just have one question --

8 A. Yes, sir.

9 Q. -- one or two

10 A. Yes, sir

11 Q. What -- I don't know exactly how to word this
12 What is the purpose of the FBI or does the FBI
13 have a mission statement or something of that
14 sort like a lot of organizations do?

15 A. Well, gosh, I don't know about a mission
16 statement. I mean, primarily we're hired to do
17 two things and that's to collect facts and
18 evidence, and we do those on a very broad
19 spectrum of investigations that are dictated by
20 laws that are on the books and we enforce
21 those. We take those facts and evidence to the
22 United States Attorney's office for prosecutive
23 opinion in most cases and that's what -- that's
24 what our mission is.

25 Q. Okay And so the FBI is a government agency;

correct?

2 A. That is correct.

And as a government agency, your purpose is to
serve as law enforcement; correct?

5 A. That's correct.

MR FISCHER: I have nothing further.

THE WITNESS: Okay.

MR HOLLIS: Nothing further.

THE WITNESS: Okay.

(The deposition concluded at 10:36

a.m.)

IN RE: Rupp vs. Phillips

I certify that I have read my testimony
and request that NO changes be made.

I certify that I have read my testimony
and request that the above changes be
made.

William R. Seck

Subscribed and sworn to before me
this ____ day of _____, 19__

Notary Public

State of _____

County of _____

My commission expires _____

MAM

IN DE	Supp	wa	Phillips																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
-------	------	----	----------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Postscript #4 Jan-July 2000

After letting time pass I decided to add new comments & observations from the last six months.

After doing the show in Portland Oregon, I became fed up with the electronic arson (damage to my CD's) so on the way to the Las Vegas show I stopped at Fallon, Nevada. This area is covered with several square miles of soil with Anthrax spores under the surface. The soil is tinged white due to the soda that saturates the soil and permits formation of spores. When I got out of my car I was observed from the road. I had pulled up along a dried up streambed and went to the bed and took a soil sample. I waved to the agents along the road and left the digging tool in the spot where I obtained the sample.

Two days later at the parking lot of the Wal-Mart in Las Vegas I was sleeping in my van. I left the windows cracked about 5 inches. At two in the morning a van marked Acculab pulled next to my van in the empty lot to within 4 inches of my door. I immediately smelled the distinct odor of culture media used to grow organisms. I wasn't sure if they were picking up or dropping off. Since it was a populated area I surmised they were only taking air samples from my van. I considered getting out and kicking a dent in the side of their vehicle and forcing a record to be made of their continuous and daily intrusions into my life but I didn't. At the gun show that weekend I told the agents that if I were actually growing Anthrax in my van I would have grown it inside of liquid plastic so that when it hardened it would seal in the spores and make them harmless to myself and others, even if there were an accident. That way I could carry around a miniature atomic bomb without worrying about hurting myself or others until I wanted to. When ready for use you only add the correct solvent to dissolve the plastic and liberate the spores. This is also a handy way of preventing the government from finding this material because you can store it as almost any type of solid as part of toys, pens, concrete, car wax, furniture, hair shampoo and so on. This was so they would not waste the "acculab" operators time or my own.

The agents continued to damage my CD duplications. I finally accidentally repeated what they were doing with my wireless phone at home. I was getting out of bed and had the phone in my left hand. I was leaning with this hand on the duplicator for support while getting up and turned on the phone. The 3 CD's I was burning instantly were bad. The machine began beeping telling me at that instant that the data stream had been interrupted and the CD's did not read back correctly. I had to be within a few inches of the duplicator with my phone in order to repeat the effect. It was obvious that Uncle Sam was using hi power equipment to do the damage in parking lots and at the gun shows to my product.

At the show in Denver, agents came up on Sunday and tried to talk me into swapping pirated software for my own CD's. I told them no because the FBI was recording every word we were saying and that I didn't need any of the software they had. I always bought the programs I needed at the store so I would get good originals. They had a new version of adobe acrobat reader on their CD and since this was free and legal I

wanted to be polite I thought I could check this out so I began to load it into my computer. One of the two agents in front of me had a funny look on his face and took off when I began to install it. Soon the other one left. They evidently did not expect me to actually do this at the show. The new reader destroyed the programs on my C drive so I could scarcely even boot my computer. I had to spend several hours reloading all my software to get it up and running again. They did this in front of many witnesses.

I told a public defender lawyer at Kansas City about this on the phone the following Monday and during our conversation a beeper came on which implied that the government was investigating this (as if they actually would). The "funny " things that were happening to my computer, CD duplicator, car, and house did stop for a few weeks but has recently started again and intensified. The appearance of legal restraint was only intended as an illusion. One of the agents at this same time also came up to me at a show and told me that the cover for my gas cap on my van can be "jimmy'd" open with a screw driver and sugar can be added to my tank. I told him that sugar doesn't damage the engine because it is an alcohol and burns with the gas. He told me yes but if you add enough the gas will not dissolve it all and it will plug the carburetor so you have to add lots of carburetor cleaner to the tank to get it dissolve enough so that it would run. This had gone on for several months each week but this also ended right after our conversation. It started again during the Civil War show trip I made in June.

This trip was a total undercover operation to the government. The first show was a Harrisburg, Penn. And was billed as an enormous event. The show hall I was located in was not air-conditioned and it was hot out. The dealers next to me and even the concession stand personnel were all undercover (many were agents I recognized from previous contact). I was in the farthest corner from the main body of the show that you could get and my sales were only a small fraction of what I expected. Over half the crowd of 2,500 that passed my booth was undercover and accounted for nearly all my sales which was disturbing to me. An interesting footnote to this show was a man who identified himself as a navy lawyer came up to talk to me. He evidently did not like what I had to say but the interesting thing I noticed is that he was under surveillance as he approached me, and the undercover agents did a small "swarm" to hear our conversation and then followed him as he walked away. These agents were also being watched by a separate party that I "felt" was not the same group.

My next show was a reenactment at Hinton, West Virginia. I set up outside and my first contact was a local called "Red" for his red hair. He and his friends immediately went to work to try and establish anti-government credibility with me. The problems were that there was no reason to bring up the anti government crap when all I was doing was sitting there working on scanning in civil war books for my CD's. It also did not help for me to recognize him personally from several gun shows in the mid-west. I was still trying to finish up a book for the show the next day at about midnight on Friday when a man "Sean" came up to me and told me that the government wanted a truce. I nearly broke out laughing. In the context of everything the government had done and continued to do this was only a sham although he may have believed it because someone told him to. I told him no. He was at the show to ostensibly videotape the governor and the next

day he did that. A woman set up near me by herself and during the setup I felt she would be making the approach. I also had the feeling that she was working with Sean and sure enough, on Saturday afternoon, an approach was made by her to form an association with me and afterwards she talked to Sean (shades of Sioux City). The undercover community keeps repeating the same techniques and practices over and over to the point where I have them all memorized and find them quite boring after three years.

My sales were poor at this show. I went to Gettysburg next. I was warned before I went that no one would be there to buy my CD's and I should consider another show. Since I had already paid and had tried hard to keep my word I decided to go to this last Civil War show anyway. It could have been named the FBI show since those were the only people there. I worked on finishing the last book for my CD and mostly tried to ignore the agents. As soon as I took a break and tried to play a video game (since the show averaged only five people in the building as customers at a time and I knew them all) the FBI began to use the swarming technique.

This is a common practice used by them for the past three years. When you cannot interrogate or harass someone who ignores you, you wait until they do things like taking a break, eating lunch, sleeping, or in this case playing a game. You send in a steady stream of agents to keep the target occupied and engaged so they cannot do what they want to relax, enjoy and so on. The effect is meant to disturb, interfere, irritate, and disorient and has been used by the military and police organizations as a mild form of psychological operations or brainwashing. After this standout incident (six agents quickly added to the five so called customers in the building-and all in front of my table) I informed them that one of the ways I could reliably tell they were agents was the use of the swarm. All I had to do the last three years was go get a hot dog in a slow stretch and could depend on taking at least 45 minutes talking to agents I already knew plus new ones I had not yet met. This allowed me to correctly identify them with 100% accuracy since this certainly is not consumer behavior. [Especially when they do not buy anything]. I also reminded them in my phone conversation home with my dad that a videotape of the FBI agents up close and personal doing this, plus a copy of the FBI and military training manuals and internal documents teaching and ordering this combined with some footage of the Oklahoma City bombing aired on CBS "60 Minutes" should set off the light bulb's in more than just a few peoples brains.

I also overheard two of the dealers comment out of earshot that they would be able to have a normal gun show the next week without me there (since this one was staged). My sales were a disaster and since it was clear that every normal activity I would engage in would become the focus of more dirty undercover operations by the government it was pointless to try and make a normal living. I decided to go back to writing weapons books and doing gun shows which is what the government wanted anyway. These agencies have been awarded \$20 Billion to try and stop the things I have published. Even in the aftermath of Oklahoma City, all these agencies have seen is sympathy, more money, more power and employees to order around. This has certainly been intoxicating to them and they no doubt want more and have actually told me so in

person. They also let me know about the task force attached to me with the "special assignment" military personnel.

I followed the disaster at Gettysburg with a gun show at Lansing Michigan with the "same old, same old" except that on Saturday night they used a loudspeaker from the park next to the fairgrounds where I was trying to sleep, to keep me awake. About every 20 minutes they would turn on the speaker and emit obnoxious noise for a few seconds, just enough to wake me up. Then they would turn it off. I was amazed someone didn't call the police. About one in the morning I had had enough. Since they have my van bugged, I told them that if they do that one more time, I will get up and drive my van around to the park and drive into them at high speed and let a Michigan jury decide who is assaulting whom (and I meant it). The loudspeaker noise ended.

I thought I would end this PS with several more basic methods of correctly identifying agents.

1. Behavior

- a) Swarming activity at shows (Bomb book buyers, Breaks, etc)
- b) Use of Signals
- c) Fake interest designed to form relationships rather than interest in commerce
- d) Team or Zone movement of agents at public events
- e) Looking at the clock or watch to see when their shift ends
- f) Oddly matched groups or pairs working together

2. Conversation

This involves a counting system best described by example. When the agents talk to the undercover dealer next to you and asks who much is this (this counts as 0), or how does it work, will they take less, and so on. These are commerce questions that are normal at a show (I worked large trade shows in my regular business before gun shows which gave me a standard for comparison)

When the following statements are made they each count as 1.

- 1. What is your name
- 2. Where are you from
- 3. Did you make these CD's yourself (no one asks the Wal-Mart clerk this)
- 4. Are you anti government like me
- 5. What do you think of _____. (Weird belief system)
- 6. How about overthrowing the government with me (so I can arrest you once I talked you into it)

Just add up the number of non product interest/buying questions and when you reach 5 the probability of an agent is 50%, at 10 it is 100%.